DEFORMATION THEORY OF GALOIS REPRESENTATIONS NOTES

Contents

Date: September 17, 2024.

Lecture 1

Useful references:

- Neukirch's *Algebraic number theory*, Chapter IV, §1 and §2.
- Neukirch, Schmidt, and Wingberg's *Cohomology of number fields*, Chapter I, §1.

1. Profinite spaces

Let $(I, \leq)$ be a directed set (i.e. an ordered set such that for any $\alpha_1, \dots, \alpha_n \in I$ there exists $\alpha \in I$ with $\alpha_i \leq \alpha$ for $i = 1, \dots, n$).

Definition 1.1. An inverse system of sets is a collection $(X_\alpha, f_{\alpha,\alpha'})_{\alpha' \leq \alpha \in I}$ with $(I, \leq)$ a directed set, X_α a set, and $f_{\alpha,\alpha'} : X_\alpha \to X_{\alpha'}$ a map whenever $\alpha' \leq \alpha$. The inverse limit (sometimes also called the projective limit) is then defined as

$$\varprojlim X_\alpha := \{(x_\alpha)_{\alpha\in I} \in \prod_I X_\alpha \mid f_{\alpha,\alpha'}(x_\alpha) = x_{\alpha'} \text{ for } \alpha' \leq \alpha\} \subset \prod_{\alpha\in I} X_\alpha$$

Furthermore,

(1) If each X_α is a topological space and each $f_{\alpha,\alpha'}$ is continuous then we say $(X_\alpha, f_{\alpha,\alpha'})_{\alpha'\leq\alpha\in I}$ is an inverse system of topological spaces. In this case $\varprojlim X_\alpha$ is equipped with the subspace topology coming from the product topology on $\prod_\alpha X_\alpha$.

(2) If each X_α is a group and each $f_{\alpha,\alpha'}$ is a group homomorphism then we say $(X_\alpha, f_{\alpha,\alpha'})_{\alpha'\leq\alpha\in I}$ is an inverse system of groups. In this case $\varprojlim X_\alpha$ is a group with multiplication defined by

$$(x_\alpha)\cdot(y_\alpha) = (x_\alpha y_\alpha)$$

(3) Similarly, if each X_α is a ring and the $f_{\alpha,\alpha'}$ are ring homomorphisms then $\varprojlim X_\alpha$ is a ring.

Remark 1.2. Open sets in the product topology on $\prod_\alpha X_\alpha$ are unions of sets of the form $\prod_\alpha U_\alpha$ where $U_\alpha \subset X_\alpha$ is open and $U_\alpha = X_\alpha$ for all but finitely many α. This is the coarsest topology (i.e the topology with the fewest open sets) making each of the projections $p_\alpha : \prod_\alpha X_\alpha \to X_\alpha$ continuous.

Exercise 1.3. Let X be a set and let $X_\alpha \subset X$ be a collection of subsets indexed by $\alpha \in I$. Make I into a directed set by putting $\alpha \leq \alpha'$ if $X_\alpha \subset X_{\alpha'}$. Then show that $(X_\alpha, f_{\alpha,\alpha'})$, where $f_{\alpha,\alpha'} : X_\alpha \to X_{\alpha'}$ is the inclusion, is an inverse system and that

$$\varprojlim X_\alpha = \bigcap_\alpha X_\alpha$$

The following exercise gives another way to think about an inverse limit:

Lemma 1.4. *The inverse limit* $\varprojlim X_\alpha$ *satisfies the following* universal property*: If* Y *is a set equipped with maps* $p_\alpha : Y \to X_\alpha$ *for each* $\alpha \in I$ *such that*

$$p_{\alpha'} = f_{\alpha,\alpha'} \circ p_\alpha$$

whenever $\alpha' \leq \alpha$ *then there is a unique map* $p : Y \to \varprojlim X_\alpha$ *such that* p_α *is the composite* $Y \to \varprojlim X_\alpha \to X_\alpha$.

Exercise 1.5. (1) Prove Lemma 1.4.

(2) Show that if $(X_\alpha, f_{\alpha,\alpha'})_{\alpha'\leq\alpha\in I}$ is an inverse system of topological spaces and Y is a topological space for which each p_α is continuous then $p : Y \to \varprojlim X_\alpha$ is continuous. Similarly, if $(X_\alpha, f_{\alpha,\alpha'})_{\alpha'\leq\alpha\in I}$ is an inverse system of groups and Y is a group with each p_α a group homomorphism then $p : Y \to \varprojlim X_\alpha$ is a group homomorphism.

Example 1.6. Let A be a ring and for $n' \leq n$ let $f_{n,n'} : A[x]/(x^n) \to A[x]/(x^{n'})$ denote the quotient map. Then $(A[x]/(x^n), f_{n,n'})$ in an inverse system over the directed set $(\mathbb{Z}_{\geq 1}, \leq)$ and there is an isomorphism of rings

$$\varprojlim A[x]/(x^n) \cong A[[x]]$$

where $A[[x]]$ denotes the power series ring over A in the variable x, i.e. the ring whose elements are formal series $\sum_{n=0}^{\infty} a_n x^n$ with $a_n \in A$.

Example 1.7. Let p be a prime number For $n' \leq n$ let $f_{n,n'} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n'}\mathbb{Z}$ denote the quotient map. Then $(\mathbb{Z}/p^n\mathbb{Z}, f_{n,n'})$ is an inverse system over the directed set $(\mathbb{Z}_{\geq 1}, \leq)$. The inverse limit is denoted $\mathbb{Z}_p$ and is called the p-adic integers.

Example 1.8. If n' divides n let $f_{n,n'} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n'\mathbb{Z}$ be the quotient map. Then $(\mathbb{Z}/n\mathbb{Z}, f_{n,n'})$ is an inverse system over the directed set $\mathbb{Z}_{\geq 1}$ which is ordered by divisibility (i.e. $n' \leq n$ is n' divides n). The inverse limit is denoted $\widehat{\mathbb{Z}}$.

Exercise 1.9. Prove that there is an isomorphism of rings

$$\widehat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p$$

where the product runs over all primes p. Hint: use the Chinese remainder theorem which asserts that for $n \in \mathbb{Z}_{\geq 1}$ with prime decomposition $n = p_1^{a_1} \dots p_m^{a_m}$ the natural map

$$\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{m} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$$

sending $a + n\mathbb{Z} \mapsto (a + p_i^{a_i}\mathbb{Z})_i$ is an isomorphism.

Definition 1.10. A topological space X is profinite if X is homeomorphic to $\varprojlim X_\alpha$ for X_α an inverse system of finite sets equipped with the discrete topology.

Proposition 1.11. *Suppose X is a Hausdorff topological space.*[1] *Then X is profinite if and only if X is compact and each $x \in X$ admits a basis of neighbourhoods consisting of open and closed subsets.*

Proof. If each X_α is finite and discrete then each X_α is compact and so $\prod_\alpha X_\alpha$ is compact by Tychonoff's theorem. Note that

$$\varprojlim X_\alpha = \bigcap_{\alpha' \leq \alpha} Y_{\alpha,\alpha'}$$

where

$$Y_{\alpha,\alpha'} = \{(x_\alpha) \in \prod_\alpha X_\alpha \mid f_{\alpha,\alpha'}(x_\alpha) = x_{\alpha'}\}$$

Each $Y_{\alpha,\alpha'}$ is the preimage of diagonal $X_{\alpha'} \subset X_{\alpha'} \times X_{\alpha'}$ under

$$\prod_\alpha X_\alpha \to X_{\alpha'} \times X_{\alpha'}, \qquad (x_\alpha) \mapsto (f_{\alpha,\alpha'}(x_\alpha), x_{\alpha'})$$

and so each $Y_{\alpha,\alpha'}$ is closed. Hence $\varprojlim X_\alpha$ is closed and so compact also. Since every subset of each X_α is open and closed it follows from Remark 1.2 that every element of $\prod_\alpha X_\alpha$ has a basis of neighbourhoods which are open and closed. The same is therefore true of $X = \varprojlim X_\alpha$.

Now we prove the converse. Let I_1 be the set of subsets $R \subset X \times X$ defining an equivalence relation, i.e.

[1] Recall that a topological space X is Hausdorff if $x_1 \neq x_2$ implies the existence of disjoint open neighbourhoors U_i of x_i with $x_1 \notin X_2$ and $x_2 \notin U_1$.

(1) $(x,y) \in R \Rightarrow (y,x) \in R$
(2) $(x,x) \in R$
(3) $(x,y),(y,z) \in R \Rightarrow (x,z) \in R$

Let $I \subset I_1$ denote the subset consisting of $R \in I_1$ for which X/R is finite and discrete for the quotient topology. Note I is an ordered set via inclusion and the X/R, together with the projections $X/R \to X/R'$ whenever $R \subset R'$, form an inverse system. By (2) of Exercise 1.4 there is a continuous map

$$p : X \to \varprojlim_{R \in I} X/R$$

Explicitly it is given by $x \mapsto (x_R)_R$ where x_R denotes the image of x in X/R. Applying the following lemma shows that p is surjective.

Lemma 1.12. *Let $p : X \to \varprojlim X_\alpha$ be a continuous map with X compact and each X_α Hausdorff. If $X \to \varprojlim X_\alpha \to X_\alpha$ is surjective for each α. Then p is surjective.*

Proof. If $(x_\alpha) \in \varprojlim X_\alpha$ then set Y_α equal to the preimage of x_α under $X \to \varprojlim X_\alpha \to X_\alpha$. This is closed since X_α is Hausdorff and so is compact since X is compact. Each Y_α is also non-empty by assumption. Furthermore, any finite intersection $Y_{\alpha_1} \cap \ldots \cap Y_{\alpha_n}$ is non-empty since it contains Y_α for any $\alpha \geq \alpha_1, \ldots, \alpha_n$. Exercise 1.13 therefore implies $\cap_{\alpha \in I} Y_\alpha$ is non-empty. Surjectivity follows since $p(x) = (x_\alpha)$ for any $x \in \cap_\alpha Y_\alpha$. □

For injectivity suppose $x_1 \neq x_2$. Since X is Hausdorf there is an open and closed neighbourhood U of x_1 not containing x_2. Then the equivalence relation R consisting of (x,y) with either $x,y \in U$ or $x,y \notin U$ is such that X/R consists of two points with the discrete topology. Furthermore, the images of x_1 and x_2 in X/R are distinct which shows $p(x_1) \neq p(x_2)$.

We conclude that $p : X \to \varprojlim_{R \in I} X/R$ is a continuous bijection between compact spaces. Any such map has a continuous inverse and so p is a homeomorphism. □

Exercise 1.13. Let X be a compact topological space and X_α a collection of closed subsets indexed by a (possibly infinite) index set I. Suppose $\cap_{i=1}^n X_{\alpha_i}$ is non-empty for any finite collection $\alpha_1, \ldots, \alpha_n \in I$. Then $\cap_{\alpha \in I} X_\alpha$ is non-empty.

Exercise 1.14. Suppose that $f : G \to H$ is continuous and injective map of profinite spaces. Show that there are injections of finite discrete spaces $f_\alpha : G_\alpha \to H_\alpha$ such that $f : G \to H$ equals

$$\varprojlim f_\alpha : \varprojlim G_\alpha \to \varprojlim H_\alpha$$

Lecture 2

Useful references:

- Neukirch's *Algebraic number theory*, Chapter IV, §1 and §2.
- Neukirch, Schmidt, and Wingberg's *Cohomology of number fields*, Chapter I, §1.

2. Profinite groups

Definition 2.1. A topological group G is a group equipped with a topology so that the map

$$G \times G \to G, \qquad (g,h) \mapsto g^{-1}h$$

is continuous. This is the same as asking that both $i : G \to G, g \mapsto g^{-1}$ and $m : G \times G \to G, (g,h) \mapsto gh$ are continuous.

Lemma 2.2. *(1) For $g \in G$ the maps $G \to G$ given by $h \mapsto hg$ and $h \mapsto gh$ are homeomorphisms.*

(2) If $U \subset G$ is open then Ug is open for every $g \in G$.

(3) If $H \subset G$ is an open subgroup then H is also closed in G.

(4) If $H \subset G$ is a subgroup then $p : G \to G/H$ is an open map for the quotient topology on G/H. Recall this means that the image $p(U)$ is open in G/H for any open $U \subset G$.

(5) G/H is Hausdorff if and only if H is closed, and G/H is discrete if and only if H is open.

(6) If G is compact and $H \subset G$ is closed then H is open if and only if G/H is finite with the discrete topology.

Proof. (1) The composite $G \to G \times G \xrightarrow{m} G$ is continuous when the first map is given by $h \mapsto (h,g)$. Likewise, if the first map is $h \mapsto (h, g^{-1})$. The same argument applies for $h \mapsto gh$.

(2) This follows directly from (1).

(3) We can write G as the disjoint union of cosets gH for $g \in G$. Since H is open each gH is open by (2). Thus $G \smallsetminus H = \bigcup_{g \notin H} gH$ is open and so H is closed.

(4) By the definition of the quotient topology $p(U)$ is open in G/H if and only if $p^{-1}(p(U))$ is open. We can write $p^{-1}(p(U)) = UH = \bigcup_{h \in H} Uh$. This is open by (2).

We leave (5) as an exercise.

(6) Using (5) we only need to show that H open implies G/H is finite. For this we note that the cosets gH form an open cover of G so compactness ensures this cover has a finite refinement. This shows G/H is finite. □

Exercise 2.3. Prove part (5) of Lemma 2.2.

Definition 2.4. A topological group G is a profinite group if it is profinite as a topological space.

Proposition 2.5. *A topological group G is profinite if and only if it is compact and the unit element $1 \in G$ admits a basis of neighbourhoods consisting of open and closed normal subgroups.*

In this case we have $G \cong \varprojlim G/H$ where H runs over the compact open normal subgroups of G.

Proof. The only if direction follows from Lemma 1.11 and (2) from Lemma 2.2. For the if direction: if G is profinite then G is compact and $1 \in G$ admits a basis of open and closed neighbourhoods by Lemma 1.11. Let U be such a neighbourhood and set

$$H' = \{h \in U \mid Uh \subset U \text{ and } Uh^{-1} \subset U\} = \{h \in U \mid Uh \subset U\} \cap \{h \in U \mid Uh^{-1} \subset U\}$$

It is easy to check that H is a subgroup of G. We claim it is open. Since $h \mapsto h^{-1}$ is a homeomorphism of G it suffices to show $H'' = \{h \in U \mid Uh \subset U\}$ is open. Note that

$$Y := \{(h_1, h_2) \in U \times U \mid h_1 h_2 \in U\}$$

is open in $G \times G$, since it is the intersection of $U \times U$ and the preimage of U under the multiplication map. Therefore, if $v \in V$ and $U_i \subset U$ is open then there exists an open neighbourhood $V_i \subset U$ of v such that $U_i V_i \subset U$. Since U is compact we can consider a finite open cover $U = \bigcup_{i=1}^n U_i$ and consider $V_v := \bigcap_i V_i$ which is an open neighbourhood in U of v. If $v' \in V_v$ then $uv' \in U$ for all $u \in U$ and so $V_v \subset H''$ which shows H'' is open. To conclude we show that the normal subgroup

$$H = \bigcap_{g \in G} gH'g^{-1} \subset H$$

it open. We have to show the union can be taken over a finite collection of $g \in G$. Note that $g_0 H' g_0^{-1} = g_1 H' g_1^{-1}$ if and only if $gH' = H'g$ for $g = g_1^{-1} g_0$. In particular, $g_0 H' g_0^{-1} = g_1 H' g_1^{-1}$ if $g_0 H' = g_1 H'$. Thus

$$H = \bigcap_{i=1}^{n} g_i H' g_i^{-1}$$

for g_i chosen so that $G = \bigcup_{i=1}^n g_i H'$.

For the last assertion let U_α be a basis of open neighbourhoods of $1 \in G$ consisting of open normal subgroups ordered by inclusion. Then there is a map $G \to \varprojlim_{U_\alpha} G/U_\alpha$ which is surjective by Lemma 1.12. Since G is Hausdorff we have $\cap_\alpha U_\alpha = \{1\}$ and so $G \to \varprojlim G/U_\alpha$ has trivial kernel. Therefore, the map is a continuous bijection between compact Hausdorff spaces. Any such map is a homeomorphism. □

Exercise 2.6. If $H \subset G$ is a subgroup of a profinite group then show that the closure of H in G is equal to the intersection of all finite index open subgroups of G which contain H.

For any topological group G we define the profinite completion

$$\widehat{G} = \varprojlim_{N} G/N$$

where the limit is taken over all finite index open normal subgroups $N \subset G$. We view $\widehat{G}$ as a profinite group. There is a continuous homomorphism $G \to \widehat{G}$.

(1) Equip $\mathbb{Z}$ with the following topology: A subset $U \subset \mathbb{Z}$ is open in the p-adic topology if and only if for each $u \in U$ there exists $n \geq 0$ such that $u + p^n\mathbb{Z} \subset U$. Show this makes $\mathbb{Z}$ into a topological group. The profinite completion of $\mathbb{Z}$ with respect to this topology is $\mathbb{Z}_p$ since the finite index open subgroups in $\mathbb{Z}$ are $p^n\mathbb{Z}$ for $n \geq 0$.

(2) The profinite completion of $\mathbb{Z}$ with respect to the discrete topology is $\widehat{\mathbb{Z}}$ since the finite index open subgroups are $n\mathbb{Z}$ for $n \geq 1$.

Exercise 2.7. Give an example of a topological group G with $\widehat{G} = \{1\}$.

Exercise 2.8. Let $G = \mathrm{SL}_n(\mathbb{Z})$ equipped with the discrete topology. Show that the natural map $G \to \prod_p \mathrm{SL}_n(\mathbb{Z}_p)$ induces a surjection

$$\widehat{f} : \widehat{G} \to \prod_p \mathrm{SL}_n(\mathbb{Z}_p)$$

Show that $\widehat{f}$ is an isomorphism if and only if every finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ is a congruence subgroup (i.e. contains $\{g \in \mathrm{SL}_n(\mathbb{Z}) \mid g \equiv 1 \text{ modulo N}\}$ for some $N > 1$.)

[For $n > 2$ every finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ is a congruence subgroup but this is not the case for $n = 2$!]

Exercise 2.9. Let G be a profinite group. Show that the power map

$$G \times \mathbb{Z} \to G, \qquad (g, n) \mapsto g^n$$

extends to a continuous map $G \times \widehat{\mathbb{Z}} \to G$ also written $(g, n) \mapsto g^n$. Show this map satisfies $g^n g^m = g^{n+m}$. and $(g^n)^m = g^{nm}$.

3. Infinite Galois theory

We now describe a source of profinite groups which will be particularly important for us. Using profinite groups we will be able to extend classical Galois theory, which usually concerns finite field extensions, to infinite extensions. First we recall the main theorem of classical Galois theory.

Definition 3.1. A field extension $K \subset L$ is algebraic if for every $x \in L$ there exists non-zero $f(X) \in K[X]$ such that $f(x) = 0$. An algebraic closure $K^a \supset K$ is a maximal algebraic extension, i.e. if $L \supset K^a$ is algebraic then $L = K^a$. Algebraic closures exist.

Let L/K be an algebraic extension. If L/K is finite then we say L/K is Galois if the group $\mathrm{Aut}(L/K)$ has order equal to the degree of L/K. In general L/K is Galois if

$$L = \bigcup_{K \subset K' \subset L} K'$$

where the union runs over finite Galois subextensions. For any Galois extension L/K we write $G(L/K) = \mathrm{Aut}(L/K)$.

Theorem 3.2 (Main theorem of Galois theory)**.** *Let $K \subset L$ be a finite Galois extension. Then*

$$H \mapsto L^H := \{x \in L \mid \sigma(x) = x \textit{ for all } h \in H\}$$

defines a bijection between the set of subgroups in G and the set of subextensions $K \subset K' \subset L$. The inverse of this bijection is given by

$$K' \mapsto \{\sigma \in G(L/K) \mid \sigma(x) = x \textit{ for all } x \in K'\} = \mathrm{Aut}(L/K')$$

Furthermore, a subgroup H in G is normal if and only if the corresponding subextension $K \subset L^H$ is Galois. In this case restriction $G(L/K) \to G(K'/K)$ induces an isomorphism

$$G(L/K)/G(L/K') \cong G(K'/K)$$

If L/K is not finite then $G(L/K)$ will no longer be a finite group. However:

Proposition 3.3. *For any Galois extension $K \subset L$ there is an isomorphism of groups*

$$G(L/K) \to \varprojlim_{K \subset L' \subset L} G(L'/K), \qquad \sigma \mapsto (\sigma|_{L'})_{L'}$$

in which the inverse limit is taken over all finite Galois subextensions and the transition maps are given by restriction.

Proof. Suppose $(\sigma_{L'}) \in \varprojlim_{K \subset L' \subset L} G(L'/K)$. Since $L = \bigcup_{K \subset L' \subset L} L'$ with the union over finite Galois L' we define an automorphism σ of L by $\sigma(x) = \sigma_{L'}(x)$ whenever $x \in L'$. This is well-defined since if $x \in L''$ then, by choosing a finite Galois extension subextension $K \subset L''' \subset L$ with $L', L'' \subset L'''$ we have

$$\sigma_{L'}(x) = \sigma_{L'''}(x) = \sigma_{L''}(x)$$

(because the transition maps $G(L'''/K) \to G(L'/K)$ and $G(L'''/K) \to G(L''/K)$ are given by restriction). Hence the map in the theorem is surjective. For injectivity note that $\sigma \in \mathrm{Aut}(L/K)$ is in the kernel if and only if $\sigma(x) = x$ for every x contained in a finite Galois subextension. As L is the union of all such subextensions it follows that $\sigma = 1$. □

Lecture 3

Useful references:

- Neukirch's *Algebraic number theory*, Chapter IV, §2 (for Galois theory)
- Atiyah–Macdonald, *Introduction to commutative algebra*, §8

4. Infinite Galois theory continued

Via the identification from Proposition 3.3 we make $G(L/K)$ into a profinite group by giving each of the finite groups $G(L'/K)$ the discrete topology.

Example 4.1. Here we see an example which shows that the bijection between subextensions $K \subset L' \subset L$ and subgroups of $G(L/K)$ given by $H \mapsto L^H$ does not extend directly to infinite extensions L/K. Take $K = \mathbb{F}_p$ and L an algebraic closure $\overline{\mathbb{F}}_p$ for a prime p. Then there is a unique degree n extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ in $\overline{\mathbb{F}}_p$. This extension is Galois and there are isomorphisms $\mathbb{Z}/n\mathbb{Z} \cong G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ sending 1 onto the automorphism of $\mathbb{F}_{p^n}$ given by $x \mapsto x^p$. Thus,

$$G(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

with $1 \in \widehat{\mathbb{Z}}$ corresponding to the automorphism $x \mapsto x^p$ of $\overline{\mathbb{F}}_p$. If $H \subset G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ denotes the subgroup corresponding to $\mathbb{Z}$ under this identification then

$$\overline{\mathbb{F}}_p^H = \{x \in \overline{\mathbb{F}}_p \mid x^p = x\} = \mathbb{F}_p = \overline{\mathbb{F}}_p^{G(\overline{\mathbb{F}}_p/\mathbb{F}_p)}$$

This shows the above map is not a bijection.

Exercise 4.2. Let L/K be a Galois extension and suppose $H, H' \subset G(L/K)$ are subgroups whose closures are equal. Show that $L^H = L^{H'}$.

Theorem 4.3. *Let L/K be a Galois extension. Then*

$$H \mapsto L^H = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}$$

defines a bijection between closed subgroups of $G(L/K)$ and subextensions $K \subset L' \subset L$. Under this bijection finite subextensions correspond to open subgroups and Galois subextensions correspond to normal subgroups.

Furthermore, if $K \subset L' \subset L$ is a Galois subextension then $G(L/K) \to G(L'/K)$ induces an isomorphism

$$G(L/K)/G(L/L') \cong G(L'/K)$$

Proof. If $K \subset L' \subset L$ is a subextension then $L' = \bigcup L''$ with the union running over finite subextensions $K \subset L'' \subset L'$. Hence $G(L/L') = \bigcap_{L''} G(L/L'')$ which is closed since each $G(L/L'')$ is closed.

If $H \subset G$ is a subgroup then $H \subset G(L/L^H)$. We will show this is an equality if H is closed. For this take $g \in G(L/L^H)$ and any finite Galois subextension $K \subset L'' \subset L$. Let H' be the image of H under the restriction map $G(L/K) \to G(L''/K)$. Since $L^H \cap L'' = (L'')^{H'}$ the main theorem of Galois theory implies that

$$H' = G(L''/L^H \cap L'')$$

In particular, the image of g in $G(L''/K)$ is contained in H'. Thus $G(L/L'')g$ and H have a common intersection. As L'' varies the $G(L/L'')g$ form a basis of open neighbourhoods of g and so, as H is closed, it follows that $g \in H$. □

5. Artinian rings

Here all rings are commutative and contain the identity.

Definition 5.1. An R-module M is Noetherian if every non-empty set $\{M_\alpha \subset M\}$ contains a maximal element, i.e. an M_α such that if $M_{\alpha'} \supset M_\alpha$ then $M_{\alpha'} = M_\alpha$. An R-module M is Artinian if every non-empty set of submodules contains a minimal element.

We say R is Noetherian (respectively Artinian) if it is Noetherian (respectively Artinian) when viewed as a module over itself.

Exercise 5.2. Show that a module M is Noetherian if and only if every submodule is finitely generated.

Proposition 5.3. *A ring R is Artinian if and only if it is Noetherian and every prime ideal in R is maximal.*

For the proof we will use the a number of lemmas:

Lemma 5.4. *If R is a field and M is a vector space over R then the following are equivalent:*

(1) M has finite dimension.
(2) M satisfies the ascending chain condition.
(3) M satisfies the descending chain condition.

Proof. This is clear. □

Corollary 5.5. *Let R be a ring such that $0 = \mathfrak{m}_1 \dots \mathfrak{m}_n$ for (not necessarily distinct) maximal ideals $\mathfrak{m}_i \subset R$. Then R is Noetherian if and only if it is Artinian.*

Proof. Note that R admits a filtration by ideals

$$0 = M_n \subset \dots \subset M_0 = R, \qquad M_i = \cap_{j=1}^{i} \mathfrak{m}_j$$

so it is enough to prove that each quotient M_i/M_{i+1} satisfies the ascending chain condition if and only if it satisfies the descending chain condition. But each M_i/M_{i+1} is an $R/\mathfrak{m}^{i+1}$-vector space so this follows from the previous lemma. □

Lemma 5.6. *If R is Artinian then every prime is maximal*

Proof. If R is Artinian and $\mathfrak{p} \subset R$ is prime then $R/\mathfrak{p}$ is also Artinian. Therefore, if $x \in R/\mathfrak{p}$ then the chain $(x) \supset (x^2) \supset \dots$ becomes stationary and so $x^n = x^{n+1}y$ for some $y \in R/\mathfrak{p}$ and some $n \geq 1$. Since $R/\mathfrak{p}$ is a domain it follows that $xy = 1$. Therefore $R/\mathfrak{p}$ is a field and $\mathfrak{p}$ is a maximal ideal. □

Lemma 5.7. *If R is Artinian then $0 = \mathfrak{m}_1 \dots \mathfrak{m}_n$ for some collection of maximal ideals $\mathfrak{m}_i \subset R$*

Proof. Since R is Artinian we can choose a minimal element J from the set of ideals obtained as a product of maximal ideals. If $\mathfrak{m} \subset R$ is maximal then $\mathfrak{m}J = J^2 = J$ by minimality. Assume $J \neq 0$. Then we can find a minimal ideal I such that $JI \neq 0$. We have $(IJ)J = IJ^2 = IJ \neq 0$. Thus minimality of I implies $IJ = I$. Minimality of I also implies $I = (f)$ for some $f \in I$. As $IJ = I$ we can write $fg = f$ for some $g \in J$. Hence $f(g-1) = 0$. However, as g is contained in every maximal ideal of R, $1 - g$ is not contained in any maximal ideal. Therefore $1 - g$ is a unit and so $f = 0$ which is a contradiction. □

Proof of Proposition 5.3. $\Rightarrow$ Lemma 5.6 shows every prime is maximal. Combining Lemma 5.7 and Corollary 5.5 shows R is Noetherian.

$\Leftarrow$ Now suppose R is Noetherian and every prime ideal is maximal. We show again that $\mathfrak{m}_1 \dots \mathfrak{m}_n = 0$ for some collection of maximal ideals in R. Then R is Artinian by Corollary 5.5. If no such product is zero then the set of ideals $I \subset R$ for which R/I is not annihilated by any finite product of maximal ideals in R is non-empty. Since R is Noetherian there is a maximal such I. We claim this implies I is prime. To show this suppose $fg \in I$ with $f, g \notin I$ and consider the exact sequence

$$0 \to R/J \xrightarrow{f} R/I \to R/I + (f) \to 0$$

where $J = \{x \in R \mid fx \in I\}$. The assumption that $f, g \notin I$ and $fg \in I$ implies both J and $I + (f)$ strictly contain I. By maximality of I it follows that both $R/I + (f)$ and R/J are killed by a finite product of maximal ideals in R. Hence R/I is also killed by such a finite product, which is a contradiction. We conclude that I is prime and hence maximal. However if I is maximal then R/I is killed by a product of maximal ideals (namely I) which again contradicts the choice of I. We conclude that $0 = \mathfrak{m}_1 \dots \mathfrak{m}_n$ for some maximal $\mathfrak{m}_i \in R$ which finishes the proof. □

Definition 5.8. A ring is *local* if it contains a unique maximal ideal.

Exercise 5.9. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Show that either $\mathfrak{m}^{n+1} \neq \mathfrak{m}^n$ for any $n \geq 0$ or that $\mathfrak{m}^n = 0$ for some $n \geq 1$. In the latter case R is Artinian.

Exercise 5.10. Show that every Artinian ring is isomorphic to a product of local Artinian rings.

Exercise 5.11. Let k be a field and A a finitely generated k-algebra (i.e. A is a quotient of $k[X_1, \dots, X_n]$). Prove that A is Artinian if and only if A is finite dimensional when viewed as a vector space over k.

Lecture 4

Useful references

(1) Atiyah–Macdonald, *Introduction to commutative algebra*, §10
(2) Eisenbud, Commutative Algebra (with a view towards algebraic geometry), §7

6. Completion of Noetherian rings

Definition 6.1. Let R be a ring and M an R-module. If $I \subset R$ is an ideal then the I-adic completion of M is the module

$$\hat{M} := \varprojlim_n M/I^n M$$

We say that M is I-adically complete if the natural map $M \to \varprojlim M/I^n M$ is an isomorphism.

Example 6.2. For a prime p, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ along the ideal (p).

Example 6.3. For any ring R the completion of $R[x_1, \dots, x_n]$ along the ideal $(x_1, \dots, x_n)$ is isomorphic to $R[[x_1, \dots, x_n]]$.

Example 6.4. Any Artin local ring is complete with respect to its maximal ideal $\mathfrak{m}$ because $\mathfrak{m}^n = 0$ for some $n \geq 1$.

If M is an I-adically complete R-module and $a_n \in I^n M$ then we can define

$$\sum_{n=0}^{\infty} a_n$$

as the preimage in M of $(0, a_1, a_1+a_2, \ldots, a_1+\ldots+a_n, \ldots) \in \varprojlim M/I^nM$. Another way of saying this is that $\hat{M}$ is complete (in the sense that Cauchy sequences converge) for the I-adic topology, i.e. the topology whose open sets are of the form $a + I^nM$ for $a \in M$ and $n \geq 0$.

Exercise 6.5. Suppose that $I, J \subset R$ are ideals and that for each $j \geq 1$ there exists $i(j) \geq 1$ such that $J^jM \subset I^{i(j)}M$. Show that the I-adic and J-adic completions of M are isomorphic

Motivation 6.6. The following example indicates the role completion plays in a geometric context. Consider the map

$$\pi : X = \{(x,y) \in \mathbb{C}^2 \mid y^2 = x + 1\} \to \mathbb{A}^1$$

given by $(x,y) \mapsto x$. Let $S = \mathbb{C}[x]$ and $R = \mathbb{C}[x,y]/(y^2 - x - 1)$ which we view as functions on $\mathbb{A}^1$ and X respectively. If $f \in S$ then we can construct $\pi^\sharp f := f \circ \pi$ which is a function on X, i.e. an element of R. This produces a homomorphism

$$\pi^\sharp : S \to R$$

which sends $x \in S$ onto $x \in R$. Since the derivative of $\pi^\sharp$ at $x = 0$, $y = -1$ is non-zero the inverse function theorem (if it applied) would say that the map π has a local inverse. However, in algebraic geometry this is not possible because there is no "local“ inverse of $\pi^\sharp$ because one would need to map $-y$ onto a square root of $x + 1$. However, such an inverse does exist if we replace $\pi^\sharp$ by the corresponding map between completions around the ideal $(x, y+1)$ because in

$$\hat{S} = \mathbb{C}[[x]]$$

there is a square root of $x + 1$ coming from the binomial expansion

$$\sqrt{x+1} = \sum_{n\geq 0} \binom{1/2}{n}(-1)^n x^n = -1 - \frac{x}{2} + \frac{x^2}{8}$$

Lemma 6.7. *Suppose that R is I-adically complete. Then $a \in R$ is a unit if and only if the image of a in R/I is a unit.*

Proof. Suppose that $ab_0 = 1 - x$ for $x \in I$. If $b_1 = \sum_{n=0}^\infty x^n \in R$ then $ab_0b_1 \equiv (1-x)(1+\ldots+x^{n-1}) = 1 - x^n \equiv 1$ modulo I^n. Therefore $ab_0b_1 - 1 \in I^n$ for every $n \geq 1$. Since R is I-adically complete $\bigcap_{n\geq 1} I^n = 0$ and so $ab_0b_1 = 1$.

□

Corollary 6.8. *If R is I-adically complete for I a maximal ideal then R is local, i.e. I is the unique maximal ideal in R.*

Proof. If $x \notin I$ then its image in R/I is non-zero and hence a unit. Therefore x is a unit by the previous lemma. It follows that any ideal $J \neq R$ in R is contained in J. □

Lemma 6.9. *Let $f : R \to S$ be a homomorphism of rings such that R is I-adically complete and S is IS-adically complete. Consider the induced maps*

$$f_n : I^n/I^{n+1} \to I^nS/I^{n+1}S$$

for $n \geq 0$. Then

(1) If f_0 is surjective then f is surjective.
(2) If f_n is injective for all n then f is injective.

Proof. (1) If f_0 is surjective then f_n is surjective for every $n \geq 0$ because if $x \in I^n S$ then $x = f(y)z$ for $y \in I^n$ and $z \in S$, and there exists $z' \in R$ such that $f(z') - z \in IS$. Hence $f(yz') - x = f(y)(f(z') - z) \in I^{n+1}S$. Now suppose $x \in S$. By surjectivity of f_0 we can find $y_1 \in R$ with $f(y_1) - x \in IS$. By surjectivity of f_1 we can find $y_2 \in I$ with $f(y_2) + f(y_1) - x \in I^2 S$. Continuing inductively we can, for each $n \geq 1$, find $y_n \in I^{n-1}$ such that

$$f(y_n) + f(y_{n-1}) - \ldots + f(y_1) - x \in I^n S$$

If $y = \sum_{n\geq 1} y_n$ then $f(y) - x = \sum_{n\geq 0} f(y_n) - x \in I^m S$ for every $m \geq 1$. Since S is I-adically complete we have $\cap_{m\geq 0} I^m S = 0$ and therefore $f(y) = x$.

(2) We claim that $R/I^n \to S/I^n S$ is injective for each $n \geq 1$. For this consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & I^n/I^{n+1} \arrow[r] \arrow[d] & R/I^{n+1} \arrow[r] \arrow[d] & R/I^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I^n S/I^{n+1}S \arrow[r] & S/I^{n+1}S \arrow[r] & S/I^n S \arrow[r] & 0
\end{tikzcd}$$

whose rows are exact. We prove the claim by induction on n. Since $R/I \to S/I$ is f_0 the case $n = 1$ is true by assumption. For the inductive step, if $R/I^n \to S/I^n S$ is injective then the two outer vertical maps in the above diagram are injective. This implies the middle vertical map is also injective (e.g. by the snake lemma). This gives injectivity of f because if $f(x) = 0$ then $x \in I^n$ for all $n \geq 0$ and hence $x = 0$. □

Theorem 6.10 (Hensel's lemma)**.** *Let R be an I-adically complete ring and suppose $f(x) \in R[x]$. If $a \in R$ is such that*

$$f(a) \equiv 0 \quad \textit{modulo} \quad f'(a)^2 I$$

where $f'(x) \in R[x]$ is the derivative of f, then there exists $b \in R$ with $f(b) = 0$ and

$$b \equiv a \quad \textit{modulo} \quad f'(a)I$$

If $f'(a)$ is a non-zerodivisor then b is unique.

For the proof we need the following lemma:

Lemma 6.11. *Let R be a ring and $f \in xR[[x]]$. Then the endomorphism*

$$\varphi : R[[x]] \to R[[x]]$$

given by $\sum r_i x^i \mapsto \sum r_i f^i$ is an isomorphism if and only if $f'(0)$ is a unit.

Proof. Since $\varphi((x^n)) \subset (x^n)$ we can consider the induced homomorphisms $\varphi_n : (x^n)/(x^{n+1}) \to (x^n)/(x^{n+1})$. Then φ is an automorphism if and only if each φ_n is. Since $f(x) \equiv f'(0)x$ modulo x^2 it follows that $f(x)^n \equiv f'(0)x^n$ modulo x^{n+1}. This shows that φ_n is given by multiplication by $f'(0)^n$, and so φ is an automorphism if and only if $f'(0)^n$ is a unit for all n, i.e. if and only if $f'(0)$ is a unit. □

Proof of Theorem 6.10. Set $f'(a) = e$. Using the Taylor expansion of f around a allows us to write

$$f(a + ex) = f(a) + f'(a)ex + h(x)(ex)^2 = f(a) + e^2 H(x)$$

for some $h(x) \in R[[x]]$ and $H(x) = x + x^2 h(x)$. Since $H'(0) = 0$ the previous lemma produces $G(x) \in R[[x]]$ with $H(G(x)) = x$. Substituting $x = G(x)$ gives

$$f(a + eG(x)) = f(a) + e^2 x$$

By hypothesis $f(a) = e^2 c$ for $c \in I$. Thus, we can evaluate the previous identity at $x = -c$ to obtain

$$f(a + eG(-c)) = 0$$

Thus, we can take $b = a + eG(-c)$.

For uniqueness suppose $b_i = a + er_i$ for $i = 1, 2$. Then

$$e^2(H(r_1) - H(r_2)) = 0$$

and so $H(r_1) = H(r_2)$. However, since $G(H(x)) = x$ it then follows that $r_1 = G(H(r_1)) = G(H(r_2)) = r_2$. □

Exercise 6.12. Use Hensel's lemma to compute the square roots of $b \in \mathbb{Z}_p^\times$ in terms of the quadratic reciprocity.

Exercise 6.13. Show that the completion of a reduced ring need not be reduced via the following example. Let $R = k[x,y]/(y^2 - x^2(x+1))$, which is a domain. Show that the completion of R at the maximal ideal (x, y) is not a domain.

Completion behaves particularly well for Noetherian rings. For example:

Theorem 6.14. *Let R be a Noetherian ring and $I \subset R$ an ideal.*

(1) The I-adic completion $\hat{R}$ of R is also Noetherian and $I^n\hat{R}$ equals the I-adic completion of the R-module I^n.

(2) If $0 \to M \to N \to P \to 0$ is an exact sequence of finitely generated R-modules then $0 \to \hat{M} \to \hat{N} \to \hat{P} \to 0$ is also exact.

Proof. See for example Proposition 10.12, 10.15 and Theorem 10.26 from Atiyah–Macdonald. □

Corollary 6.15. *Let R be a Noetherian ring and $I = (a_1, \dots, a_n)$ an ideal of R. If $\hat{R}$ denotes the I-adic completion then*

$$R[[x_1, \dots, x_n]]/(x_1 - a_1, \dots, x_n - a_n) \cong \hat{R}$$

Proof. Take the $(x_1, \dots, x_n)$-adic completion of the exact sequence $0 \to (x_1, \dots, x_n) \to R[x_1, \dots, x_n] \xrightarrow{f} R \to 0$ of $R[x_1, \dots, x_n]$-modules where f is given by $x_i \mapsto a_i$. By (2) Theorem 6.14 this sequence stays exact. By (1) the I-adic completion of I is $(x_1 - a_1, \dots, x_n - a_n) \subset R[[x_1, \dots, x_n]]$ which gives the isomorphism. □

7. Complete local Noetherian rings

Recall that a ring R if local if it contains a unique maximal ideal $\mathfrak{m}$. The residue field of such a ring is then $R/\mathfrak{m}$.

Definition 7.1. A complete discrete valuation ring is a complete Noetherian local ring whose maximal ideal is principal and generated by a non-nilpotent element.

Theorem 7.2 (Cohen Structure Theorem)**.** *Let R be a complete local Noetherian ring with maximal ideal $\mathfrak{m}$. Then there exists an isomorphism*

$$\mathcal{O}[[x_1,\dots,x_n]]/I \xrightarrow{\sim} R$$

where $\mathcal{O}$ is either a field, or a discrete valuation ring with maximal ideal generated by a prime number p.

Proof, assuming the existence of coefficient rings. We begin with the following definition: a subring $\mathcal{O} \subset R$ is a coefficient ring if

1. the induced map $\mathcal{O}/\mathfrak{m} \cap \Lambda \to R/\mathfrak{m}$ is an isomorphism.
2. Λ is a local ring complete with respect to $\mathcal{O} \cap \mathfrak{m}$, which is generated by p where p equals the characteristic of $R/\mathfrak{m}$.

Note that if $R/\mathfrak{m}$ has characteristic zero then $\mathcal{O}$ is a field and if p is not nilpotent in R then $\mathcal{O}$ is a discrete valuation ring. The difficult part of the theorem is the following two facts:

Fact 7.3. Every complete local ring contains a coefficient ring.

Proof. See Tags 0328,0329 and 032A from the Stacks project. □

Let us show how to prove the theorem assuming these facts. Let $\mathcal{O} \subset R$ be a coefficient ring and suppose $a_1,\dots,a_n$ generate the maximal ideal of R. Then there is a homomorphism

$$\mathcal{O}[[x_1,\dots,x_n]] \to R$$

given by $x_i \mapsto a_i$. This homomorphism is surjective modulo the ideal $(x_1,\dots,x_n)$ and so is surjective itself. □

Lecture 5

Useful references

- Serre's "Local fields“, §4 and 5.

8. Construction of coefficient rings

We are going to prove the existence of coefficient rings (i.e. Fact 7.3) in two cases which are most important for us, namely when the complete local Noetherian ring has finite residue field or residue field of characteristic p. These constructions will be based on the following application of Hensel's lemma:

Lemma 8.1. *Suppose that R is a ring complete with respect to a maximal ideal $\mathfrak{m}$ and that $f(X) \in R[X]$ is such that its image $\overline{f}(X) \in R/\mathfrak{m}[X]$ has a simple root $\overline{a} \in \overline{f}(X)$, i.e. $\overline{f}(\overline{a}) = 0$ and $\overline{f}'(\overline{a}) \neq 0$. Then there exists a unique $a \in R$ with $f(a) = 0$ and $\overline{a} = a$ modulo $\mathfrak{m}$.*

Proof. Choose $a_0 \in R$ lifting $\overline{a}$. Then $f'(a_0)$ is a unit in R because its image in the residue field is non-zero. Applying Hensel's lemma produces a unique a as claimed. □

Proposition 8.2. *Suppose that $R/\mathfrak{m}$ has characteristic zero. Then there exists a coefficient ring (in this case a field) $\mathcal{O} \subset R$.*

Proof. Since the composite $\mathbb{Z} \to R \to R/\mathfrak{m}$ is non-zero so is $\mathbb{Z} \to R$. Therefore this map extends to an embedding $\mathbb{Q} \to R$. y Zorn's lemma there is then a maximal subfield $K \subset R$. We claim that $K \to R \to R/\mathfrak{m}$ is an isomorphism.

We first show that $K \to R/\mathfrak{m}$ is an algebraic extension. If not there would exist $\overline{x} \in R/\mathfrak{m}$ transcendental over K. Choose $x \in R$ lifting $\overline{x}$ and consider the map $S[X] \to R$ given by $X \mapsto a$. This must be an injection since any polynomial in the kernel would contradict the transcendence of $\overline{x}$ over K. Hence, the field of rational functions $S(X)$ embeds into R contradicting the maximality of K.

Therefore, if $\overline{x} \in R/\mathfrak{m}$ then there is a minimal polynomial $f \in K[X]$ with $f(\overline{x}) = 0$ in $R/\mathfrak{m}$. Since $R/\mathfrak{m}$ has characteristic zero the polynomial f has no repeated roots. Therefore Lemma 8.1 shows there exists $x \in R$ with $f(x) = 0$. Hence $K[x] \to R$ is a subfield in R which equals K by maximality. Thus $x \in K$ and hence $K \cong R/\mathfrak{m}$. □

Next we consider the mixed characteristic setting in an easy case:

Proposition 8.3. *Suppose that R is a complete Noetherian local ring maximal ideal $\mathfrak{m}$ and finite residue field. Then there exists a coefficient ring.*

Proof. Let p denote the characteristic of $k = R/\mathfrak{m}$. Then $pR \subset \mathfrak{m}$ and so R is p-adically complete. Considering the p-adic completion of $\mathbb{Z} \to R$ gives a map

$$\mathbb{Z}_p \to R$$

Since is $R/\mathfrak{m}$ is finite it is a separable extension of $\mathbb{F}_p$ and so $k = \mathbb{F}_p(\alpha)$ for some $\alpha \in k$ which is a simple root of its minimal polynomial over $\mathbb{F}_p$. If $\widetilde{f}(X) \in R[X]$ lifts $f(X)$ then, by Lemma 8.1, there is a unique $\widetilde{\alpha} \in R$ lifting α with $\widetilde{f}(\widetilde{\alpha}) = 0$. Thus, there is a map

$$\mathcal{O} := \mathbb{Z}_p[X]/(\widetilde{f}(X)) \to R$$

given by $X \mapsto \widetilde{\alpha}$. We claim that $\mathcal{O}$ is a coefficient ring for R. For this note that, if $\widetilde{\alpha}$ has degree n then there is an isomorphism of $\mathbb{Z}_p$-modules

$$\mathbb{Z}_p^n \to \mathcal{O}$$

given by $(x_0, \ldots, x_{n-1}) \mapsto x_0 + x_1 X + \ldots x_{n-1} X^{n-1}$. This shows that $\mathcal{O}$ is p-adically complete. It also shows that $\mathcal{O}/p\mathcal{O}$ is a degree n extension of $\mathbb{F}_p$ containing k. It must therefore equal k. □

In both cases we saw that separability was important. In fact

Lemma 8.4. *Let k be a field of characteristic $p > 0$ and suppose that $x \mapsto x^p$ is surjective. If $f(X) \in k[X]$ is an irreducible polynomial and $f(x) = 0$ for $x \in k$ then x is a simple root of $f(X)$.*

Proof. If x is not a simple root of $f(X)$ then $f'(x) = 0$. It follows that

$$f(X) = \sum f_i X^{ip}$$

for some $f_i \in k$. Since $x \mapsto x^p$ is surjective we have

$$f(X) = g(X)^p, \qquad g(X) = \sum_i f_i^{1/p} X^i$$

which contradicts the irreducibility of f. □

Proposition 8.5. *Suppose that R is an $\mathfrak{m}$-adically complete ring with $p \in \mathfrak{m}$ and $R/\mathfrak{m}$ is perfect, i.e. $x \mapsto x^p$ is surjective. Then there exists a unique multiplicative map*

$$R/\mathfrak{m} \to R$$

such that the composition $R/\mathfrak{m} \to R \to R/\mathfrak{m}$ is an bijection. If $pR = 0$ then this map is also additive.

Proof. For any $\overline{x} \in R/\mathfrak{m}$ choose $\overline{x}_n$ such that $\overline{x}_n^{p^n} = \overline{x}$ and choose $x_n \in R$ lifting $\overline{x}_n$. We need the following lemma

Lemma 8.6. *If $a \equiv b$ modulo $\mathfrak{m}^n$ and $p \in \mathfrak{m}$ then $a^p \equiv b^p$ modulo $\mathfrak{m}^{n+1}$.*

Proof. The binomial theorem gives $a^p - b^p = (b-(b-a)^p) - b^p = \sum \binom{p}{n} b^n (b-a)^{p-n} \in \mathfrak{m}^2$. □

Since $x_{n+1}^p \equiv x_n$ modulo $\mathfrak{m}$ it follows that $x_{n+1}^{p^{n+1}} \equiv x_n^{p^n}$ modulo $\mathfrak{m}^n$. Therefore we can consider

$$x = \lim_{n\to\infty} x_n^{p^{n+1}} = (x_1^p, x_2^{p^2}, \dots) \in \varprojlim R/\mathfrak{m}^n$$

Let us show that x does not depend upon the choice of lifts x_n. If x_n' are another choice then since $x_n \equiv x_n'$ modulo $\mathfrak{m}$ and the lemma gives that $x_n^{p^n} \equiv x_n'^{p^n}$ modulo $\mathfrak{m}^{n+1}$. This shows that x is independent of the choice of x_n and so $\overline{x} \mapsto x$ gives a homomorphism

$$R/\mathfrak{m} \to R, \qquad \overline{x} \mapsto x$$

as claimed. To see that it is unique suppose $f_1, f_2 : R/\mathfrak{m} \to R$ are two such homomorphisms. Then for each $x \in R/\mathfrak{m}$ one has

$$f_1(x^{1/p^n}) \equiv f_2(x^{1/p^n}) \text{ modulo } \mathfrak{m}$$

and so, using the lemma, we have $f_1(x) = f_1(x^{1/p^n}) \equiv f_2(x^{1/p^n})^{p^n} = f_2(x)$ modulo $\mathfrak{m}^{n+1}$. This is true for all $n \geq 1$ and so $f_1(x) = f_2(x)$. □

Corollary 8.7. *Suppose that R is a complete local Noetherian ring with $pR = 0$ for a prime p. Then R admits a coefficient field.*

The construction of $\mathcal{O}$ in the previous proposition is a special case of a more general construction of Witt vectors:

Theorem 8.8. *Let k be a perfect field of characteristic p. Then there exists a complete discrete valuation ring $W(k)$ with maximal ideal generated by p and $W(k)/pW(k) = k$. This ring is universal in the following sense.*

Furthermore, this ring is uniquely determined in the following sense: for any complete discrete valuation ring R with maximal ideal generated by p and any isomorphism $\overline{f} : R/(p) \to k$ there exists a unique isomorphism $fR \to W(k)$ such that $f \equiv \overline{f}$ modulo p.

Lecture 6

9. Categories and functors

Definition 9.1. A (locally small) category $\mathcal{C}$ consists of the following data:

1. a collection of objects
2. for any two objects X and Y a set of morphisms $\mathrm{Hom}_{\mathcal{C}}(X, Y)$
3. for every object X an element $1_X \in \mathrm{Hom}(X, X)$
4. for any three objects X, Y, Z a composition map

$$\circ : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

   such that
   - these composition maps are associative, i.e. $(f \circ g) \circ h = f \circ (g \circ h)$
   - $f \circ 1_X = f$ and $1_Y \circ f = f$ for any $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

We write $f : X \to Y$ is $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$. A morphism $f : X \to Y$ is an isomorphism if there exists an inverse $g : Y \to X$ such that $g \circ f = 1_X$ and $f \circ g = 1_Y$.

Exercise 9.2. Show that if f is an isomorphism then the inverse g is unique.

Example 9.3. The category $\underline{\mathrm{Set}}$ is the category whose objects are sets and whose morphisms $f : X \to Y$ are maps of sets. The morphism $1_X : X \to X$ is the identity and the composition maps are given by the usual composition of functions.

Example 9.4. The category $\underline{\mathrm{Group}}$ is the category whose objects are groups and whose morphisms $f : G \to H$ are group homomorphisms. Again, the morphism $1_X : X \to X$ is the identity and the composition maps are given by the usual composition of functions.

Similarly, we can define the categories $\underline{\mathrm{Ring}}$ and for a ring R the category $\underline{\mathrm{Mod}}_R$.

Example 9.5. Let X be a topological space. Then there is a category $\mathrm{Open}(X)$ whose objects are open subsets U of X and whose morphisms $f : U \to U'$ are inclusions.

Example 9.6. Let G be a group. Then we can view $\underline{G}$ as a category with a single object $*$, with $\mathrm{Hom}_{\underline{G}}(*, *) = G$, and with composition given by multiplication in the group and the identity morphism given by $1 \in G$.

Example 9.7. For a ring S let $\underline{\mathrm{Alg}}_S$ denote the category whose objects are S-algebras, i.e. rings R equipped with a homomorphism $S \to R$, and whose morphisms are S-algebra homomorphisms, i.e. homomorphisms of rings $f : R \to R'$ such that

$$\begin{tikzcd}
S \arrow[r] \arrow[d] & R \arrow[dl] \\
R' &
\end{tikzcd}$$

commutes.

Definition 9.8. A category $\mathcal{C}'$ of a category $\mathcal{C}$ is a subcategory if every object of $\mathcal{C}'$ is an object of $\mathcal{C}$ and if $\mathrm{Hom}_{\mathcal{C}'}(X,Y) \subset \mathrm{Hom}_{\mathcal{C}}(X,Y)$ for every pair of objects X, Y in $\mathcal{C}'$. A subcategory is full if

$$\mathrm{Hom}_{\mathcal{C}'}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(X,Y)$$

for every pair of objects X, Y in $\mathcal{C}'$.

Example 9.9. Let $\underline{\mathrm{Mod}}_R^{fg}$ denote the category of finitely generated R-modules. Then $\underline{\mathrm{Mod}}_R^{fg}$ is a full subcategory of $\underline{\mathrm{Mod}}_R$.

Example 9.10. Let $\underline{\mathrm{Ab}}$ denote the category of abelian groups. Then $\underline{\mathrm{Ab}}$ is a full subcategory of $\underline{\mathrm{Group}}$.

Example 9.11. Let S be a ring. Then $\underline{\mathrm{Alg}}_S$ is a subcategory (but not a full subcategory) of $\underline{\mathrm{Mod}}_S$.

Definition 9.12. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A covariant functor $F : \mathcal{C} \to \mathcal{D}$ is given by attaching an object $F(X)$ to every object X in $\mathcal{C}$ and by giving maps

$$F : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$$

such that

(1) $F(f) \circ F(g) = F(f \circ g)$.
(2) $F(1_X) = 1_{F(X)}$.

A contravariant functor is defined in the same way except that the directions of arrows are reversed so that F sends a morphism $f : X \to Y$ to

$$F(f) : F(Y) \to F(X)$$

Thus, a contravariant functor $F : \mathcal{C} \to \mathcal{D}$ is given by attaching an object $F(X)$ in $\mathcal{D}$ to every object X in $\mathcal{C}$ and by giving maps

$$F : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(F(Y), F(X))$$

such that

(1) $F(f) \circ F(g) = F(f \circ g)$.
(2) $F(1_X) = 1_{F(X)}$.

If F is a functor $\mathcal{C} \to \mathcal{D}$ and G is a functor $\mathcal{C} \to \mathcal{E}$ then we write $F \circ G$ for their composition.

Example 9.13. The is a forgetful covariant functor $\underline{\text{Group}} \to \underline{\text{Set}}$ which sends a group G onto its underlying set and which sends a group homomorphism $f : G \to H$ onto $f : G \to H$ viewed as a map of sets.

Example 9.14. Let $f : R \to S$ be a homomorphism of rings. Then there is a covariant functor $f_* : \underline{\text{Mod}}_S \to \underline{\text{Mod}}_R$ which sends an S-module M onto the R-module with underlying set M and with R-action given by

$$r \cdot_R m := f(r) \cdot_S m, \qquad r \in R, m \in M$$

Definition 9.15. Suppose that $F, G : \mathcal{C} \to \mathcal{D}$ are two covariant functors. Then a morphism $\alpha : F \to G$ of functors is a family of morphisms $\alpha : F(X) \to G(X)$ in $\mathcal{D}$ for every object X in $\mathcal{C}$ such that the following diagram commutes

$$\begin{tikzcd}
F(X) \arrow[r, "F(f)"] \arrow[d, "\alpha(X)"] & F(Y) \arrow[d, "\alpha(Y)"] \\
G(X) \arrow[r, "G(f)"] & G(Y)
\end{tikzcd}$$

for every morphism $f : X \to Y$. One defines a morphism between contravariant functors similarly.

This allows us to form the category $\underline{\text{Fun}}_{\text{co}}(\mathcal{C}, \mathcal{D})$ whose objects are covariant functors $F : \mathcal{C} \to \mathcal{D}$ and whose morphisms are given by morphisms $\alpha : F \to G$. Similarly, one can define the category $\underline{\text{Fun}}_{\text{contra}}(\mathcal{C}, \mathcal{D})$ of contravariant functors.

Definition 9.16. Let $F : \mathcal{C} \to \mathcal{D}$ be a covariant functor.

(1) F is essentially surjective if for every object X in $\mathcal{D}$ there exists an object Y in $\mathcal{C}$ and an isomorphism $f : F(Y) \to X$ in $\mathcal{D}$.
(2) F is fully faithful if $F : \text{Hom}_{\mathcal{C}}(X, Y) \to \text{Hom}_{\mathcal{D}}(F(X), F(Y))$ is an isomorphism for every pair of objects $X, Y \in \mathcal{C}$.
(3) A functor is an equivalence if it is essentially surjective and fully faithful.

Similarly for contravariant functors.

Lemma 9.17. *A functor $F : \mathcal{C} \to \mathcal{D}$ is an equivalence if and only if it admits a quasi inverse, i.e. a functor $G : \mathcal{D} \to \mathcal{C}$ such that*

$$F \circ G \equiv \text{id}_{\mathcal{D}}, \qquad F \circ G \equiv \text{id}_{\mathcal{C}}$$

in $\underline{\text{Fun}}(\mathcal{D}, \mathcal{D})$ and $\underline{\text{Fun}}(\mathcal{C}, \mathcal{C})$.

10. Some categorical constructions

Many constructions we are used to in sets, groups, rings, etc. can be formulated for categories. However, in a general category objects need not be sets so one cannot necessarily manipulate with elements. Instead, one makes constructions via a universal property. We have already seen an example of this for inverse limits:

Recollection 10.1. The inverse limit $\varprojlim X_\alpha$ over a directed set I satisfies the following *universal property*: If Y is a set equipped with maps $p_\alpha : Y \to X_\alpha$ for each $\alpha \in I$ such that

$$p_{\alpha'} = f_{\alpha,\alpha'} \circ p_\alpha$$

whenever $\alpha' \leq \alpha$ then there is a unique map $p : Y \to \varprojlim X_\alpha$ such that p_α is the composite $Y \to \varprojlim X_\alpha \to X_\alpha$.

This allows us to make sense of the notion of an inverse limit to any category. In fact one make an even more general definition if one replaces the directed set (recall we defined this as a partially ordered set for which any finite collection of elements admitted a common upper bound) with just a partially ordered set. In this case we obtain the notion of a limit:

Definition 10.2. Let I be a partially ordered set and $\mathcal{C}$ a category. Let $(X_\alpha, f_{\alpha,\alpha'})$ be an inverse system over I, i.e. a collection of objects X_α in $\mathcal{C}$ and a collection of morphisms $f_{\alpha,\alpha'} : X_\alpha \to X_{\alpha'}$ whenever $\alpha' \leq \alpha$ such that $f_{\alpha,\alpha} = 1_{X_\alpha}$ and

$$f_{\alpha',\alpha''} \circ f_{\alpha,\alpha'} = f_{\alpha,\alpha''}$$

whenever $\alpha'' \leq \alpha' \leq \alpha$. Then the limit $\varprojlim X_\alpha$ is an object of $\mathcal{C}$ admitting morphisms $f_\alpha : \varprojlim X_\alpha \to X_\alpha$ such that

$$f_{\alpha,\alpha'} \circ f_\alpha = f_{\alpha'}$$

for every $\alpha' \leq \alpha$, and which is universal for this property in the following sense: if Y is an object of $\mathcal{C}$ admitting morphisms $y_\alpha : Y \to X_\alpha$ with

$$f_{\alpha,\alpha'} \circ y_\alpha = y_{\alpha'}$$

for all $\alpha' \leq \alpha$ then there exists a unique morphism $y : Y \to \varprojlim X_\alpha$ such that $y \circ f_\alpha = y_\alpha$ for every α.

We emphasise that the limit $\varprojlim X_\alpha$ may not exist.

Exercise 10.3. Show that if $\varprojlim X_\alpha$ exists then it is unique up to unique isomorphism, i.e. if X_1, X_2 both satisfy the universal property then there exists a unique isomorphism $X_1 \to X_2$ in $\mathcal{C}$.

Clearly the notion of a limit encapsulates the notion of inverse limits which we say before. However, by allowing general partially ordered sets we also obtain new constructions:

Exercise 10.4. Let I be a set with the discrete order, i.e. $\alpha \leq \alpha'$ if and only if $\alpha = \alpha'$. Then an inverse system over I is just a collection of objects indexed by I. Show that in $\underline{\mathrm{Set}}$ one has

$$\varprojlim_{\alpha \in I} X_\alpha = \prod X_\alpha$$

Another particular example of a limit which is very important is the notion of a fibre product.

Definition 10.5. Let $I = \{x, y, z\}$ be the partially ordered set with $x \leq y, x \leq z$ and no non-trivial order relations. Then an inverse system over I in a category $\mathcal{C}$ consists of three objects X, Y, Z in $\mathcal{C}$ and a pair of morphisms

$$\begin{tikzcd}
Y \arrow[dr, "f"] & & Z \arrow[dl, "g"] \\
& X &
\end{tikzcd}$$

The limit of this system (if it exists) is called the fibre product and is denoted

$$Y \times_X Z = Y \times_{X,f,g} Z$$

Exercise 10.6. Show that fibre product of two maps $f : Y \to X$ and $g : Z \to X$ of sets exists in $\underline{\mathrm{Set}}$ and is given by

$$Y \times_X Z = \{(y, z) \in Y \times Z \mid f(y) = g(z)\}$$

Most of the categories we will consider have objects consisting of sets equipped with some additional data, e.g. the structure of a group, or a ring, or a topological space. For these categories there is a forgetful functor into $\underline{\mathrm{Set}}$; it forgets this extra data. We have already seen that the formation of inverse limits often commutes with these operations. For example if $\underline{\mathrm{Top}}$ is the category of topological spaces with morphisms between continuous maps then the forgetful functor

$$F : \underline{\mathrm{Top}} \to \underline{\mathrm{Set}}$$

commutes with the formation of inverse limits, i.e.

$$F(\varprojlim X_\alpha) = \varprojlim F(X_\alpha)$$

Similarly for inverse limits of groups or topological groups. However for a general functor $F : \mathcal{C} \to \mathcal{D}$ there is only a morphism

$$F(\varprojlim X_\alpha) \to \varprojlim F(X_\alpha)$$

which will not always be an isomorphism. Nevertheless, there is one useful condition which ensures it is an isomorphism:

Proposition 10.7. *Let $F : \mathcal{C} \to \mathcal{D}$ be a functor and assume that F admits a left adjoint $G : \mathcal{D} \to \mathcal{C}$, i.e. a functor for which there exist bijections*

$$f_{X,Y} : \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \to \mathrm{Hom}_{\mathcal{D}}(F(X), Y)$$

which are functorial in the sense that if $X \to X'$ is a morphism in $\mathcal{C}$ then the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \arrow[r, "f_{X,Y}"] \arrow[d] & \mathrm{Hom}_{\mathcal{D}}(F(X), Y) \arrow[d] \\
\mathrm{Hom}_{\mathcal{C}}(X', G(Y)) \arrow[r, "f_{X',Y}"] & \mathrm{Hom}_{\mathcal{D}}(F(X'), Y)
\end{tikzcd}$$

commutes, and similarly for any morphism $Y \to Y'$. Then

$$F(\varprojlim X_\alpha) \to \varprojlim F(X_\alpha)$$

is an isomorphism for any limit in $\mathcal{C}$.

Example 10.8. A left adjoint G to a forgetful map $F : \mathcal{C} \to \underline{\text{Set}}$ can often be constructed by setting $G(X)$ equal to the object of $\mathcal{C}$ "freely" generated by the set X. For example, suppose $\mathcal{C} = \underline{\text{Alg}}_R$. Then define $G : \underline{\text{Set}} \to \underline{\text{Alg}}_R$ by setting $G(X)$ equal to the polynomial ring

$$R[T_x]_{x \in X}$$

and, for $f : X \to Y$ a map of sets, setting $F(f) : R[T_x]_{x \in X} \to R[T_y]_{y \in Y}$ equal to the R-algebra homomorphism sending $T_x \mapsto T_{f(x)}$. It is easy to see that G is a left adjoint to F.

11. Yoneda's lemma

Every object X in a category $\mathcal{C}$ defines a covariant functor

$$h_X : \mathcal{C} \to \underline{\text{Set}}$$

which on objects is given by $h_X(Y) = \text{Hom}_{\mathcal{C}}(X, Y)$ and on morphisms sends $f_Y : Y \to Y'$ onto

$$h_X(f_Y) : \text{Hom}_{\mathcal{C}}(X, Y) \xrightarrow{g \mapsto f_Y \circ g} \text{Hom}_{\mathcal{C}}(X, Y')$$

If $f_X : X \to X'$ and $f_Y : Y \to Y'$ are morphisms in $\mathcal{C}$ then we also obtain commuting diagrams

$$\begin{tikzcd}
h_{X'}(Y) \arrow[r, "h_X(f_Y)"] \arrow[d, "h \mapsto h \circ f_X"] & h_{X'}(Y') \arrow[d, "h \mapsto h \circ f_X"] \\
h_X(Y) \arrow[r, "h_{X'}(f_Y)"] & h_X(Y')
\end{tikzcd}$$

(the commuting of the diagram comes down to associativity of composition). It follows that these vertical maps define a morphism of functors

$$h_{X'} \to h_X$$

In other words $X \mapsto h_X$ defines a contravariant functor

$$\mathcal{C} \to \widehat{\mathcal{C}} := \underline{\text{Fun}}_{co}(\mathcal{C}, \underline{\text{Set}})$$

Lemma 11.1 (Yoneda's lemma)**.** *The functor $h_X : \mathcal{C} \to \widehat{\mathcal{C}}$ is essentially surjective for every object X in $\mathcal{C}$.*

Proof. We have to show that the map

$$\text{Hom}_{\mathcal{C}}(X, X') \to \text{Hom}_{\widehat{\mathcal{C}}}(h_{X'}, h_X)$$

which sends $f : X \to X'$ onto the morphism of functors $h_f : h_{X'} \to h_X$ defined by

$$h_{X'}(Y) \xrightarrow{h \mapsto h \circ f} h_X(Y), \qquad Y \text{ an object in } \mathcal{C}$$

is a bijection. For injectivity, suppose $f, g : X \to X'$ are morphisms with $h \circ f = h \circ g$ for every $h \in \text{Hom}_{\mathcal{C}}(Y, X)$ and every object Y in $\mathcal{C}$. Then, taking $X' = Y$ and

$h = 1_{X'}$, it follows that $f = g$. For surjectivity, suppose $\alpha : h_{X'} \to h_X$ is a morphism of functors. Then, for any $f_Y : Y \to Y'$ we have a commuting diagram

$$\begin{tikzcd}
h_{X'}(Y) \arrow[r, "g \mapsto f_Y \circ g"] \arrow[d, "\alpha(Y)"] & h_{X'}(Y') \arrow[d, "\alpha(Y')"] \\
h_X(Y) \arrow[r, "g \mapsto f_Y \circ g"] & h_X(Y')
\end{tikzcd}$$

Now take $Y = X'$ so that $f_Y : X' \to Y' \in h_X(Y')$ and consider the image of $1_{X'}$ around this diagram. This gives

$$\alpha(Y')(f_Y) = \alpha(Y')(1_{X'} \circ f_Y) = \alpha(X')(1_{X'}) \circ f_Y$$

Therefore $\alpha(Y') = h_{\alpha(X')(1_{X'})}$ which proves surjectivity. □

Definition 11.2. We say that a pair (X, ι) represents a covariant functor $F : \mathcal{C} \to \underline{\text{Set}}$ if

$$\iota : F \to h_X$$

is an isomorphism of functors in $\widehat{\mathcal{C}}$.

Lecture 7

12. Representable functors

Recall from last time that if $\mathcal{C}$ is a category and X is an object of $\mathcal{C}$ then there is a functor

$$h_X : \mathcal{C} \to \underline{\text{Set}}$$

given by $h_X(Y) = \text{Hom}_{\mathcal{C}}(X, Y)$.

Definition 12.1. A functor $F : \mathcal{C} \to \underline{\text{Set}}$ is representable if there exists an object X in $\mathcal{C}$ and an isomorphism of functor

$$u : h_X \xrightarrow{\sim} F$$

We say that F is represented by (F, u).

Recall that having an isomorphism of functors $u : h_X \cong F$ is the same as having, for every object Y in $\mathcal{C}$, bijections of sets

$$u : (Y)\,\text{Hom}_{\mathcal{C}}(X, Y) \to F(Y)$$

which are functorial in Y.

Proposition 12.2. *For any functor $F : \mathcal{C} \to \underline{\text{Set}}$ there is a bijection*

$$\text{Hom}_{\text{Fun}}(h_X, F) \xrightarrow{\sim} F(X)$$

given by $u \mapsto u(X)(1_X)$.

Proof. An inverse is given by $x \mapsto u_x$ where u_x is the morphism of functors $u_x(Y) : \text{Hom}_{\mathcal{C}}(X, Y) \to F(Y)$ given by $u_x(f) = F(f)(x)$. To check this is actually an inverse involves the same calculations that we used to prove Yoneda's lemma last time. □

Taking $F = h_Y$ recovers Yoneda's lemma.

Corollary 12.3. *Let $F : \mathcal{C} \to \underline{\text{Set}}$ be a functor. Then the following data is equivalent.*

1. *An isomorphism of functors $h_X \cong F$*
2. *An object $x^{\text{univ}} \in F(X)$ such that the map*
$$\text{Hom}_{\mathcal{C}}(X, Y) \to F(Y)$$
given by $f \mapsto F(f)(x^{\text{univ}})$ is a bijection for every Y.

Thus we can also say that a functor F is represented by a pair (X, x^{univ}) with $x^{\text{univ}} \in F(X)$. Yoneda's lemma implies this pair is unique up to isomorphism.

Example 12.4. Let $F : \underline{\text{Ring}} \to \underline{\text{Set}}$ be the forgetful functor $F(R) = R$ viewed as a set. Then F is representable by the pair $(\mathbb{Z}[x], x)$ because for every ring R and $r \in R$ there exists a unique homomorphism of rings $f : \mathbb{Z}[x] \to R$ with $f(x) = r$.

Example 12.5. Let $F : \underline{\text{Ring}} \to \underline{\text{Set}}$ be the functor $F(R) = R^\times$ (units in R). Then F is represented by the pair $(\mathbb{Z}[x, x^{-1}], x)$ because for every ring R and $r \in R^\times$ there exists a unique homomorphism $f : \mathbb{Z}[x, x^{-1}] \to R$ with $f(x) = r$.

Example 12.6. Let $f \in \mathbb{Z}[x]$ be a polynomial and consider the functor $F : \underline{\text{Ring}} \to \underline{\text{Set}}$ given by $F(R) = \{x \in R \mid f(x) = 0\}$. Then F is represented by the pair
$$(\mathbb{Z}[x]/(f(x)), x)$$
because for every $r \in R$ with $f(r) = 0$ there exists a unique ring homomorphism $\mathbb{Z}[x]/(f(x)) \to R$ with $x \mapsto r$.

Example 12.7. Let $f(x) \in \mathbb{Z}[x]$. Then the functor $F : \underline{\text{Ring}} \to \underline{\text{Set}}$ given by $F(R) = \{r \mid f(r) \in R^\times\}$ is representable by
$$(\mathbb{Z}[x, \frac{1}{f(x)}], x)$$

Exercise 12.8. Let $f_1, \dots, f_n, g_1, \dots, g_p \in \mathbb{Z}[x_1, \dots, x_m]$. Show that the functor $F : \underline{\text{Ring}} \to \underline{\text{Set}}$ with
$$F(R) = \{(x_1, \dots, x_m) \in R^m \mid f_i(x_1, \dots, x_m) = 0, g_j(x_1, \dots, x_m) \in R^\times \text{ for all } i, j\}$$
is representable.

Example 12.9. Here is an example of a functor which is not representable. Let $F : \underline{\text{Ring}} \to \underline{\text{Set}}$ be given by $F(R) = \{x \in R \mid x = y^2 \text{ for some } y \in R\}$. Then F is not representable. To see this suppose F was represented by (X, x_2) with $x_2 = x_1^2$. Then for every ring R with a square r there exists a unique homomorphism $f : X \to R$ with $r = f(x_2)$. If $R = \mathbb{Z}[x]$ and $r = x^2$ then we can compose f with the automorphism σ of $\mathbb{Z}[x]$ given by $x \mapsto -x$ to obtain $f' : X \to R$ with $r = f'(x_2)$. Hence $f' = f$. However, $f(x_1) = \pm x$ and so $f'(x_1) = \mp x$ which contradicts the fact that $f' = f$.

Example 12.10. Let R be a complete local ring and let $\mathcal{C}$ denote the category of complete local R-algebras. Then the functor $F : \mathcal{C} \to \underline{\text{Set}}$ given by $F(A) = \mathfrak{m}_A$ the maximal ideal in A is represented by

$$(R[[x]], x)$$

because for every complete local R-algebra A and every $m \in \mathfrak{m}_A$ there is a unique homomorphism $f : R[[x]] \to A$ of R-algebras such that $f(x) = m$.

Example 12.11. Here is a less useful example. Let Top^{op} be the opposite category of topological spaces and consider the functor

$$\text{Top}^{\text{op}} \to \underline{Set}$$

sending a topological space $(X, \mathcal{T}_X)$ onto $\mathcal{T}_X$ (i.e. the set of open subsets). Then this is representable by the topological space $X = \{0,1\}$ with topology given by $\{\varnothing, \{1\}, \{0,1\}\}$. Indeed, the map

$$\text{Hom}(Y, X) \to \mathcal{T}_Y$$

given by $f \mapsto f^{-1}(\{1\})$ has inverse sending $U \in \mathcal{T}_Y$ onto the characteristic function of U.

Exercise 12.12. Let R be a ring such that $h_R(k) = \text{Hom}_{\underline{\text{Ring}}}(R, k)$ is a finite set for every field k. Show that R is Artinian.

The following is a toy example of the kind of functors we will be interested in. Let G be a finite group and for $n \geq 1$ consider the functor

$$\text{Rep}_G^{\square} : \underline{\text{Ring}} \to \underline{\text{Set}}$$

which sends a ring R onto the set of homomorphisms $G \to \text{GL}_n(R)$, i.e. the set of R-representations of G.

Lemma 12.13. *This functor is representable by a quotient R_G of $\mathbb{Z}[x_1, \dots, x_N]$ for some $N \geq 0$.*

Proof. Write $G = \{g_1, \dots, g_d\}$ and set $S_G = \mathbb{Z}[X_l^{ij}]$ for $1 \leq l \leq d$ and $1 \leq i, j \leq n^2$. Define a map

$$\widetilde{\rho} : G \to \text{GL}_n(S_G)$$

by $g_l \mapsto (X_l^{ij})_{ij}$. Set $I \subset S_G$ equal the ideal whose elements are generated by the entries of $\widetilde{\rho}(g)\widetilde{\rho}(g')\widetilde{\rho}(gg')^{-1}$ for every $g, g' \in G$ and $R_G = S_G/I$. Then the composite

$$\rho^{\text{univ}} : G \xrightarrow{\widetilde{\rho}} \text{GL}_n(S_G) \to \text{GL}_n(R_G)$$

is a homomorphism. The pair $(R_G, \rho^{\text{univ}})$ represents $\text{Rep}_G^{\square}$ because any homomorphism $\rho : G \to \text{GL}_n(R)$ produces a homomorphism $S_G \to R$ given by $X_l^{ij} \mapsto \rho(g_l)_{ij}$ and since ρ is a homomorphism I is contained in the kernel of this homomorphism we obtain an induced homomorphism $R_G \to R$. □

Next we take a field k and $\rho : G \to \mathrm{GL}_n(k)$. Let $\mathcal{C}$ denote the category of complete local rings with residue field k whose morphisms are maps $R \to S$ for which

$$\begin{tikzcd} R \arrow[rr] \arrow[dr] & & S \arrow[dl] \\ & k & \end{tikzcd}$$

commute. Then we can consider the functor of deformations

$$D_\rho^\square : \underline{\mathrm{Ring}\,/R} \to \underline{\mathrm{Set}}$$

which sends A onto the set of $\rho' \in \mathrm{Rep}_G^\square(A)$ for which the composite

$$G \xrightarrow{\rho'} \mathrm{GL}_n(A) \to \mathrm{GL}_n(A/\mathfrak{m}_A)$$

equals ρ.

Proposition 12.14. *Let $x_\rho : R_G \to k$ be the homomorphism corresponding to ρ and let $\mathfrak{m}_\rho$ be the kernel. Assume x_ρ is surjective. Then the functor $D_\rho^\square$ is representable by*

$$\widehat{R}_G = \varprojlim R_G/\mathfrak{m}_\rho^n$$

Proof. Let A be a complete local ring with residue field k. For any $f : R_G \to A$ write $\rho_f : G \to \mathrm{GL}_n(A)$ for the corresponding representation. Then

$$\rho_f \in D_\rho^\square(A) \Leftrightarrow R_G \to A \to A/\mathfrak{m}_A \text{ equals } x_\rho \Leftrightarrow \mathfrak{m}_A \supset \mathfrak{m}A$$

Therefore, if $\rho_f \in D_\rho^\square(A)$ then $\mathfrak{m}$-adically completing $R_G \to A$ gives $\widehat{R}_G \to \widehat{A} = A$. Conversely, for any morphism $\widehat{R}_G \to A$ in $\mathcal{C}$ the composite $R_G \to \widehat{R}_G \to A$ corresponds to an element of $D_\rho^\square$. Therefore

$$D_\rho^\square \cong \mathrm{Hom}_{\mathcal{C}}(\widehat{R}_G, A)$$

which proves the claim. □

Lecture 8

13. Framed deformations of a profinite group

Let G be a profinite group and k a finite field of characteristic p and recall the ring of Witt vectors $W(k)$, i.e. the unique complete discrete valuation ring with residue field k and maximal ideal generated by p.

Definition 13.1. Let $\mathcal{C}$ denote the category of complete Noetherian local $W(k)$ with residue field k whose morphisms are ring homomorphisms $R \to S$ such that

$$\begin{tikzcd} R \arrow[rr] \arrow[dr] & & S \arrow[dl] \\ & k & \end{tikzcd}$$

commutes. For any $A \in \mathcal{C}$ we write $\mathfrak{m}_A$ for the maximal ideal in A.

Definition 13.2. For any object A in $\mathcal{C}$ a framed A-representation of G is a continuous homomorphism

$$\rho : G \to \mathrm{GL}_n(A)$$

Here we equip $\mathrm{Mat}_{n\times n}(A) \cong A^{n\times n}$ with the $\mathfrak{m}_A$-adic topology and $\mathrm{GL}_n(A)$ with the subspace topology.

Lemma 13.3. *Let $\rho : G \to \mathrm{GL}_n(A)$ be a homomorphism with $A \in \mathcal{C}$. Then the following are equivalent:*

(1) ρ is continuous

(2) For every $n \geq 1$ the composite $\rho_m : G \xrightarrow{\rho} \mathrm{GL}_n(A) \to \mathrm{GL}_n(A/\mathfrak{m}_A^m)$ factors through a finite quotient of G.

Proof. If ρ is continuous then so is ρ_m and hence the preimage of $1 \in \mathrm{GL}_n(A/\mathfrak{m}_A^m)$ is open in G and therefore has finite index. For the converse, condition (ii) implies that each ρ_m is continuous. Since

$$\mathrm{GL}_n(A) = \varprojlim_m \mathrm{GL}_n(A/\mathfrak{m}_A^m)$$

the universal property of the inverse limit produces a continuous homomorphism $\varprojlim \rho_m : G \to \mathrm{GL}_n(A)$ which coincides with ρ modulo $\mathfrak{m}_A^m$ for every $m \geq 0$. It follows these homomorphisms are equal.

□

Definition 13.4. Let $\overline{\rho} : G \to \mathrm{GL}_n(k)$ be a framed representation of G. For every $A \in \mathcal{C}$ set

$$D^{\square}_{\overline{\rho}}(A) = \{\text{framed representations } \rho : G \to \mathrm{GL}_n(A) \mid G \xrightarrow{\rho} \mathrm{GL}_n(A) \to \mathrm{GL}_n(\mathbb{F}) = \overline{\rho}\}$$

Then $A \mapsto D^{\square}_{\overline{\rho}}$ defines a functor $D^{\square}_{\overline{\rho}} : \mathcal{C} \to \underline{\mathrm{Set}}$.

Theorem 13.5. *Assume that every open subgroup $G_0 \subset G$ satisfies the following* p-finiteness condition*:*

- *There are only finitely many continuous homomorphisms $G_0 \to \mathbb{F}_p$.*

Then $D^{\square}_{\overline{\rho}} : \mathcal{C} \to \underline{\mathrm{Set}}$ is representable by a quotient of $W(k)[[X_1, \dots, X_N]]$ for some $N \geq 0$.

Before giving the proof we need to discuss the relevance of the p-finiteness condition.

Definition 13.6. A finite group is a p-group if its cardinality is a power of p. A profinite group is pro-p if every finite quotient is a p-group.

Definition 13.7. The pro-p-completion $G^{(p)}$ of a profinite group G is defined as $\varprojlim_U G/U$ where U runs over all open normal subgroups for which G/U is a p-group. The natural map $G \to G^{(p)}$ is surjective and every continuous homomorphism $G \to H$ with H a pro-p-group factors through $G^{(p)}$.

Lemma 13.8. *The following are equivalent:*

(1) The are only a finite number of continuous homomorphisms $G \to \mathbb{F}_p$.

(2) $G^{(p)}$ *is topologically finitely generated, i.e. there exists* $\gamma_1, \ldots, \gamma_n \in G^{(p)}$ *which generate a dense subgroup of* G.

Proof. We can assume that $G = G^{(p)}$ and so G is pro-p. For any profinite group let $\Phi(G)$ denote the intersection of all maximal proper open subgroups in G. The quotient of a p-group by a maximal proper subgroup must be isomorphic to $\mathbb{F}_p$ and so the same is true for any pro-p group. Hence $G/\Phi(G)$ is an inverse limit of abelian groups isomorphic to $\mathbb{F}_p$. This shows that $G/\Phi(G)$ is an $\mathbb{F}_p$-vector space. Condition (1) is therefore equivalent to asking that $G/\Phi(G)$ is finite.

If $\gamma_1, \ldots, \gamma_n$ topologically generate G then their images generate $G/\Phi(G)$ and so $G/\Phi(G)$ must be finite. For the converse, choose $\gamma_1, \ldots, \gamma_n$ in G whose images generate $G/\Phi(G)$. Set H equal to the closure of the subgroup generated by $\gamma_1, \ldots, \gamma_n$. If $H \neq G$ then we can find a maximal open proper subgroup $H \subset H' \subset G$. But also $\Phi(G) \subset H'$, which contradicts the fact that the closure of the subgroup generated by H and $\Phi(G)$ is G. □

Proposition 13.9. *Suppose that* G *satisfies the* p*-finiteness condition. Then there exists a closed subgroup* $H \subset G$ *such that* G/H *is topologically generated and every* $\rho : G \to \mathrm{GL}_n(A)$ *factors through* G/H.

Proof. Set $G_0 = \ker \overline{\rho}$. If $\rho \in D^{\square}_{\overline{\rho}}(A)$ then $\rho|_{G_0} : G_0 \to \mathrm{GL}_n(A)$ factors through K_1 where K_i for $i \geq 1$ are defined by

$$K_i = \ker\left(\mathrm{GL}_n(A) \to \mathrm{GL}_n(A/\mathfrak{m}_A^i)\right)$$

Note that the K_i for $i \geq 1$ form a basis of open neighbourhoods of K_1 and that $X \mapsto 1 - X$ defines a bijection

$$K_i/K_{i+1} \cong \mathrm{Mat}_{n\times n}(\mathfrak{m}_A^i/\mathfrak{m}_A^{i+1})$$

This shows that K_1 is a pro-p-group and so $\rho'|_{G_0} : G_0 \to \mathrm{GL}_n(A)$ factors through $G_0^{(p)}$. Let $H_0 = \ker(G_0 \to G_0^{(p)})$ and set

$$H = \bigcap_{g \in G/G_0} gH_0g^{-1}$$

Note that since H_0 is normal in G_0 the subgroup gH_0g^{-1} only depends upon the class of g in G/G_0, so this intersection makes sense. We also see that H is normal in G because if $g' \in G$ then

$$g'Hg'^{-1} = \bigcap_{g \in G/G_0} g'gH_0g^{-1}g'^{-1} = \bigcap_{g'' \in G/G_0} g''H_0g''^{-1} = H$$

Lastly, since G/G_0 is finite the intersection is finite and so H is closed in G and open in H_0. From the exact sequence $1 \to H_0/H \to G_0/H \to G_0/H_0 \to 0$ and the fact that G_0/H_0 is topologically finitely generated we see that G_0/H is topologically finitely generated. The upshot is that every $\rho \in D^{\square}_{\overline{\rho}}(A)$ factors through G/H for H an open normal subgroup with G/H topologically finitely generated, as required. □

Lecture 9

14. Representing framed deformations

We continue the discussion from the previous lecture. Recall we fixed k a finite field and denoted $\mathcal{C}$ the category of complete local Noetherian rings with residue field k. Morphisms are homomorphisms inducing the identity on k. We also write $\mathcal{C}^0$ for the full subcategory of $\mathcal{C}$ whose objects are Artinian. Recall, every object of $\mathcal{C}$ is a $W(k)$-algebra. For any profinite group G and $\overline{\rho} : G \to \mathrm{GL}_n(k)$ we have the functor

$$D_{\overline{\rho}}^{\square} : \mathcal{C} \to \underline{\mathrm{Set}}$$

sending a ring A onto the set of homomorphisms $\rho : G \to \mathrm{GL}_n(A)$ whose composite $G \to \mathrm{GL}_n(A) \to \mathrm{GL}_n(k)$ equals $\overline{\rho}$. We saw before that $D_{\overline{\rho}}^{\square}$ is representable when G is a finite group.

Lemma 14.1. *Suppose G is finite and generated by $g_1, \dots, g_m$, and $(R_{\overline{\rho}}^{\square}, \rho^{\mathrm{univ}})$ represents $D_{\overline{\rho}}^{\square}$. Then $R_{\overline{\rho}}^{\square}$ is generated over $W(k)$ by the entries of $\rho^{\mathrm{univ}}(g_l)$ for $l = 1, \dots, m$.*

Proof. Let S be the subring of $R_{\overline{\rho}}^{\square}$ generated by the entries of the $\rho^{\mathrm{univ}}(g_l)$. Then $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R_{\overline{\rho}}^{\square})$ factors through $\mathrm{GL}_n(S)$. By the universality of $(R_{\overline{\rho}}^{\square}, \rho^{\mathrm{univ}})$ there must be a unique homomorphism $s : R_{\overline{\rho}}^{\square} \to S$ giving $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(S)$. Moreover, the composite

$$s' : R_{\overline{\rho}} \xrightarrow{s} S \to R_{\overline{\rho}}$$

must be the identity since $s' \circ \rho = \rho$. Therefore $s(r) = r$ for every $r \in R_{\overline{\rho}}$ and so $S = R_{\overline{\rho}}$. □

Recall $\mathcal{C}^0 \subset \mathcal{C}$ is the full subcategory whose objects are Artinian.

Definition 14.2. Consider a pair (R, ρ) with R a local $W(k)$-algebra with residue field k and $\rho : G \to \mathrm{GL}_n(R)$ a continuous homomorphism whose composite $G \to \mathrm{GL}_n(R) \to \mathrm{GL}_n(k)$ equals $\overline{\rho}$. Then we say (R, ρ) pro-represents $D_{\overline{\rho}}^{\square}$ if the map

$$\mathrm{Hom}(R, A) \to D_{\overline{\rho}}^{\square}$$

given by $f \mapsto G \xrightarrow{\rho} \mathrm{GL}_n(R) \to \mathrm{GL}_n(A)$ is a bijection for every $A \in \mathcal{C}^0$.

Lemma 14.3. *Suppose that $R \in \mathcal{C}$ and (R, ρ) pro-represents $D_{\overline{\rho}}^{\square}$. Then (R, ρ) represents $D_{\overline{\rho}}^{\square}$.*

Proof. Obviously if (R, ρ) is a representing pair then they also pro-represent. For the converse, suppose $A \in \mathcal{C}$ and $\rho_A \in D_{\overline{\rho}}(A)$. Set $\rho_{A,i} : G \to \mathrm{GL}_n(A) \to \mathrm{GL}_n(A/\mathfrak{m}_A^i)$. Then for each i there exists a unique homomorphism $f_i : R \to A/\mathfrak{m}_A^i$ so that $\rho_{A,i}$ equals the composite

$$G \xrightarrow{\rho} \mathrm{GL}_n(R) \to \mathrm{GL}_n(A/\mathfrak{m}_A^i)$$

In particular we see that $R \xrightarrow{f_i} A/\mathfrak{m}_A^i \to A/\mathfrak{m}_A^{i+1}$ equals f_{i+1}. Since A is $\mathfrak{m}_A$-adically complete we have $A = \varprojlim A/\mathfrak{m}_A^i$ and so the f_i produce a homomorphism $R \to A$ with the property that the composite

$$G \xrightarrow{\rho} \mathrm{GL}_n(R) \to \mathrm{GL}_n(A)$$

is $\equiv \rho_A$ modulo $\mathfrak{m}_A^i$ for every $i \geq 0$. In other words, this composite equals ρ_A whose proves that (R, ρ) represents $D_{\overline{\rho}}^{\square}$. □

Proposition 14.4. *Let G be a profinite group. Then $D_{\overline{\rho}}^{\square}$ is pro-representable by a pair (R, ρ).*

Proof. Write $G = \varprojlim_U G/U$ for open normal subgroups $U \subset G$ with $U \subset \ker \overline{\rho}$. This means that $\overline{\rho} : G \to \mathrm{GL}_n(k)$ factors through

$$\overline{\rho}_U : G/U \to \mathrm{GL}_n(k)$$

For each U let (R_U, ρ_U) be the pair representing $D_{\overline{\rho}_U}^{\square}$. Note that if $U \subset U'$ then we can view $\rho_{U'} : G/U' \to \mathrm{GL}_n(R_{U'})$ as a representation $\rho_{U'} : G/U \to G/U' \to \mathrm{GL}_n(R_{U'})$. Therefore, we obtain homomorphisms

$$R_U \to R_{U'}$$

such that $\rho_{U'}$ is obtained as the composite

$$G/U' \to G/U \xrightarrow{\rho_U} \mathrm{GL}_n(R_U) \to \mathrm{GL}_n(R_{U'})$$

This allows us to define a homomorphism

$$\rho : G \to \varprojlim \mathrm{GL}_n(R_U) = \mathrm{GL}_n(\varprojlim_U R_U)$$

Set $R = \varprojlim_U R_U$. We claim (R, ρ) pro-represents $D_{\overline{\rho}}^{\square}$. To see this take $A \in \mathcal{C}^0$ and suppose $\rho_A \in D_{\overline{\rho}}^{\square}(A)$. Since A is Artinian the group $\mathrm{GL}_n(A)$ is finite and so ρ_A factors through G/U for some open normal $U \subset G$. Therefore, we obtain a homomorphism $R_U \to A$ such that

$$G \xrightarrow{\rho_U} \mathrm{GL}_n(R_U) \to \mathrm{GL}_n(A)$$

equals ρ_A. Hence ρ_A is the image of $R \to R_U \to A$ under the map

$$\mathrm{Hom}(R, A) \to D_{\overline{\rho}}^{\square}(A)$$

This shows surjectivity. For injectivity suppose $f_1, f_2 : R \to A$ are such that $x_i : G \xrightarrow{\rho} \mathrm{GL}_n(A) \xrightarrow{f_i} \mathrm{GL}_n(A)$ are equal. We can choose an open normal $U \subset G$ such that x_1, x_2 both factor through G/U. Therefore both f_1, f_2 factor through $R \to R_U$ and since R_U represents $D_{\overline{\rho}_U}^{\square}$ it follows that $f_1 = f_2$. □

Proposition 14.5. *Suppose that G is topologically finitely generated. Then $D_{\overline{\rho}}^{\square}$ is representable by a quotient of a power series ring over $W(k)$.*

Proof. Let (R,ρ) be the pro-representing pair from the previous proposition. We claim that if $g_1,\dots,g_m$ topologically generate then R is generated over $W(k)$ by the entries of $\rho^{\text{univ}}(g_l)$. Let $S \subset R$ be the subring they generate. Note that S is a quotient of a power series ring over $W(k)$. Therefore (the additive group of) S is profinite and so, since each R_U is complete and hence Hausdorff for the $\mathfrak{m}_U$-adic topology, to show that $S = R$ it suffices to show $S \to R \to R_U$ is surjective for every U (see Lemma 1.12). But $g_1,\dots,g_n$ topologically generate G if and only if their images generate G/U for every open normal subgroup $U \subset G$. The claimed surjectivity therefore follows from Lemma 14.1. □

This finishes the proof of Theorem 13.5 from the previous lecture.

15. Tangent spaces

Definition 15.1. Let $F : \mathcal{C}^0 \to \underline{\text{Set}}$ be a functor. The tangent space of F is defined as

$$F(k[\epsilon])$$

where $k[\epsilon] = k[\epsilon]/(\epsilon^2)$.

Proposition 15.2. *There are following sets are in bijection:*

(1) $D^{\square}_{\overline{\rho}}(k[\epsilon])$

(2) The set $Z^1(G, \text{End}(\overline{\rho}))$ *of* 1*-cocycles, i.e. functions* $f : G \to \text{Mat}_{n\times n}(k)$ *such that* $f(gh) = \overline{\rho}(g)f(h) + f(g)\overline{\rho}(h)$ *for all* $g,h \in G$.

(3) The set of homomorphisms $\rho : G \to \text{GL}_{2n}(k)$ *of the form*

$$\rho(g) = \begin{pmatrix} \overline{\rho}(g) & F(g) \\ 0 & \overline{\rho}(g) \end{pmatrix}$$

for some $F(g) \in \text{Mat}_{n\times n}(k)$.

(4) $\text{Hom}_k(\mathfrak{m}_R/\mathfrak{m}_R^2 + pR, k)$ *for* $\mathfrak{m}_R$ *the maximal ideal in a pro-representing pair* (R,ρ) *of* $D^{\square}_{\overline{\rho}}$.

Furthermore, the natural k-vector space structures on the sets in (2) and (4) coincide under these bijections.

Proof. Note that a map $G \to \text{GL}_{2n}(k)$ given by

$$g \mapsto \begin{pmatrix} \overline{\rho}(g) & F(g) \\ 0 & \overline{\rho}(g) \end{pmatrix}$$

is a homomorphism if and only if

$$\begin{pmatrix} \overline{\rho}(g) & F(g) \\ 0 & \overline{\rho}(g) \end{pmatrix}\begin{pmatrix} \overline{\rho}(h) & F(h) \\ 0 & \overline{\rho}(h) \end{pmatrix} = \begin{pmatrix} \overline{\rho}(gh) & \overline{\rho}(g)F(h) + F(h)\overline{\rho}(g) \\ 0 & \overline{\rho}(gh) \end{pmatrix} = \begin{pmatrix} \overline{\rho}(gh) & F(gh) \\ 0 & \overline{\rho}(gh) \end{pmatrix}$$

i.e. if and only if $F(gh) = \overline{\rho}(g)F(h) + F(h)\overline{\rho}(g)$. Therefore the bijection between the sets in (2) and (3) is given by $f \in Z^1(G,\overline{\rho})$ onto the homomorphism

$$g \mapsto \begin{pmatrix} \overline{\rho}(g) & f(g) \\ 0 & \overline{\rho}(g) \end{pmatrix}$$

For the bijection between the sets in (1) and (2) notice that there every element of $\mathrm{GL}_n(k[\epsilon])$ can be written as

$$g + \epsilon F$$

with $g \in \mathrm{GL}_n(k)$ and $F \in \mathrm{Mat}_{n\times n}(k)$. Therefore, if $\rho \in D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ we can write $\rho(g) = \overline{\rho}(g) + \epsilon F_\rho(g)$ for some function $F_\rho : G \to \mathrm{Mat}_{n\times n}(k)$. The fact that ρ is a homomorphism is equivalent to

$$(\overline{\rho}(g) + \epsilon F_\rho(g))(\overline{\rho}(h) + \epsilon F_\rho(h)) = \overline{\rho}(gh) + \epsilon F_\rho(gh)$$

i.e. that $F_\rho(g)\overline{\rho}(h) + \overline{\rho}(g)F_\rho(h) = F_\rho(gh)$. Hence $\rho \mapsto F_\rho$ gives a bijection between $D^{\square}_{\overline{\rho}}(k[\epsilon])$ and $Z^1(G, \overline{\rho})$.

Finally, we give a bijection between $D^{\square}_{\overline{\rho}}(k[\epsilon])$ and $\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR)$. By definition of pro-representability we have

$$D^{\square}_{\overline{\rho}}(k[\epsilon]) = \mathrm{Hom}(R, k[\epsilon])$$

where the homomorphism on the right are those inducing the identity on residue fields. Any such homomorphism f must send $\mathfrak{m}_R$ onto the maximal ideal (ϵ) of $k[\epsilon]$ and p onto zero, and so induces a map $\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR) \to (\epsilon) = k$ of k-vector spaces. Conversely, given a map $f : \mathfrak{m}_R/(\mathfrak{m}_R^2 + pR) \to k$ of k-vector spaces we can define a homomorphism $R \to k[\epsilon]$ by $r \mapsto \overline{r} + \epsilon f(r - [\overline{r}])$ where $[\cdot]$ denotes the Teichmuller lifting $k \to W(k)$. □

Exercise 15.3. Check that the natural k-vector space structures on $Z^1(G, \overline{\rho})$ and $\mathrm{Hom}(\mathfrak{m}_R/(\mathfrak{m}_R^2 + pR), k)$ coincide whenever (R, ρ) pro-represents $D^{\square}_{\overline{\rho}}$.

Proposition 15.4. *If G satisfies the p-finiteness condition, i.e. if $\mathrm{Hom}(G_0, \mathbb{F}_p)$ is finite for every open subgroup $G_0 \subset G$ then*

$$D^{\square}_{\overline{\rho}}(k[\epsilon])$$

is finite.

Proof. We show that $Z^1(G, \overline{\rho})$ is finite. Take $G_0 = \ker \overline{rho}$. Then the restriction of any $f \in Z^1(G, \overline{\rho})$ to G_0 is a homomorphism

$$G_0 \to \mathrm{Mat}_{n\times n}(k)$$

If this restriction is the zero function then F induces a well defined function $G/G_0 \to \mathrm{Mat}_{n\times n}(k)$ which we can view as an element of $Z^1(G/G_0, \overline{\rho})$. Therefore, we can an exact sequence

$$0 \to Z^1(G/G_0, \mathrm{Mat}_{n\times n}(k)) \to Z^1(G, \mathrm{Mat}_{n\times n}(k)) \to \mathrm{Hom}(G_0, \mathrm{Mat}_{n\times n}(k))$$

The left hand term is finite since G/G_0 and $\mathrm{Mat}_{n\times n}(k)$ are both finite. The p-finiteness hypothesis implies the right most term is also finite. Hence $Z^1(G, \overline{\rho})$ is finite as claimed.

For another proof note that if G satisfies the p-finiteness condition then $D^{\square}_{\overline{\rho}}$ is pro-represented by a Noetherian local ring R and hence $\mathfrak{m}_R/\mathfrak{m}_R^2$ is finite dimensional. □

Lecture 10

Useful references

- Gouvea's "Galois deformation theory" notes, Lecture 3

16. Unframed deformations

Maintain the notation from the previous lecture. Thus

- G is a profinite group and j is field
- $\mathcal{C}$ is the category of complete local Noetherian rings with residue field k and morphisms are ring homomorphisms compatible with the map into k
- $\mathcal{C}^0$ is the full subcategory of $\mathcal{C}$ of Artinian rings

Definition 16.1. Let $\overline{\rho} : G \to \mathrm{GL}_n(k)$ be a continuous homomorphism. Then, for $A \in \mathcal{C}$, define

$$D_{\overline{\rho}}(A) = D_{\overline{\rho}}^{\square}(A)/\sim$$

where $\sim$ denotes the following equivalence relation on $D_{\overline{\rho}}(A)^{\square}$: we have $\rho_1 \sim \rho_2$ if and only if there exists

$$h \in \ker\left(\mathrm{GL}_n(A) \to \mathrm{GL}_n(k)\right)$$

such that $\rho_1(g) = h \circ \rho_2(g) \circ h^{-1}$ for all $g \in G$.

Lemma 16.2. *$D_{\overline{\rho}} : \mathcal{C} \to \underline{\mathrm{Set}}$ is a functor.*

Proof. Suppose $\rho_1, \rho_2 \in D_{\overline{\rho}}^{\square}(A)$ represent the same element of $D_{\overline{\rho}}(A)$ so that $\rho_1(g) = h\rho_2(g)h^{-1}$ for all $g \in G$. If $f : A \to B$ is a morphism in $\mathcal{C}$ then also write $f : \mathrm{GL}_n(A) \to \mathrm{GL}_n(B)$ for the induced map. Then $f(\rho_i) = f \circ \rho_i$ and so $f(\rho_1)(g) = f(h)f(\rho_2)f(h)^{-1}$. Thus $f(\rho_1)$ and $f(\rho_2)$ represent the same element in $D_{\overline{\rho}}(A)$. □

If R is a local ring with residue field k and $\rho : G \to \mathrm{GL}_n(R)$ is a continuous homomorphism then we say (R, ρ) pro-represent $D_{\overline{\rho}}$ if the map

$$\mathrm{Hom}(R, A) \to D_{\overline{\rho}}(A)$$

which sends $f : R \to A$ onto the equivalence class of the composite $G \xrightarrow{\rho} \mathrm{GL}_n(R) \to \mathrm{GL}_n(A)$ is a bijection for every $A \in \mathcal{C}^0$. Note that if (R, ρ) pro-represent $D_{\overline{\rho}}^{\square}$ then this pair *does not* represent $D_{\overline{\rho}}$ because the map $D_{\overline{\rho}}^{\square}(A) \to D_{\overline{\rho}}(A)$ is never a bijection.

Lemma 16.3. *If (R, ρ) pro-represent $D_{\overline{\rho}}$ and $R \in \mathcal{C}$ then $D_{\overline{\rho}}$ is represented by $(R, [\rho])$ where $[\rho]$ denotes the equivalence class of ρ in $D_{\overline{\rho}}(R)$.*

Proof. The key is to prove that $D_{\overline{\rho}}$ is continuous, i.e. that

$$D_{\overline{\rho}}(A) = \varprojlim_i D_{\overline{\rho}}(A/\mathfrak{m}_A^i)$$

for any $A \in \mathcal{C}$. There is a natural map $D_{\overline{\rho}}(A) \to \varprojlim_i D_{\overline{\rho}}(A/\mathfrak{m}_A^i)$. For surjectivity, an element of $\varprojlim_i D_{\overline{\rho}}(A/\mathfrak{m}_A^i)$ corresponds to a collection of $\rho_i \in D_{\overline{\rho}}^{\square}(A/\mathfrak{m}_A^i)$ and $F_i \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_A)$ such that

$$F_i^{-1}\rho_i F_i \equiv \rho_{i-1} \text{ modulo } \mathfrak{m}_A^{i-1}$$

Set $F^i = \prod_{j>i} F_j \in 1 + \mathrm{Mat}(\mathfrak{m}_A)$ (note this infinite product converges by completeness of A). Then

$$F^i\rho_i(F^i)^{-1} \equiv (F^i)F_i\rho_{i-1}F_i^{-1}(F^{i+1})^{-1} = F^{i-1}\rho_{i-1}(F^{i-1})^{-1} \text{ modulo } \mathfrak{m}_A^{i-1}$$

so $\rho_i' := F^i\rho_i(F^i)^{-1}$ is a compatible sequence $\varprojlim D_{\overline{\rho}}^{\square}(A/\mathfrak{m}_A^i)$ which gives $\rho \in D_{\overline{\rho}}^{\square}$ whose equivalence class in $D_{\overline{\rho}}$ maps onto our systems of classes in $\varprojlim_i D_{\overline{\rho}}(A/\mathfrak{m}_A^i)$.

For injectivity, suppose $\rho_1, \rho_2 \in D_{\overline{\rho}}^{\square}(A)$ define the same equivalence class modulo $\mathfrak{m}_A^i$ for every i. Then there exist $F_i \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_A^i)$ such that $F_i\rho_1F_i^{-1} \equiv \rho_2$ modulo $\mathfrak{m}_A^i$ for all i. If $F = \prod_{i\ge 1} F_i \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_A)$ then $F\rho_1F^{-1} = \rho_2$ so $[\rho_1] = [\rho_2]$ in $D_{\overline{\rho}}(A)$. □

Definition 16.4. For $\rho \in D_{\overline{\rho}}^{\square}(A)$ set

$$C_A(\rho) := \{P \in \mathrm{Mat}_{n\times n}(A) \mid P\rho(g) = \rho(g)P \text{ for all } g \in G\}$$

The set $C_A(\overline{\rho})$ controls how well behaved $D_{\overline{\rho}}$ is.

Theorem 16.5 (Mazur, Ramakrishna)**.** *If $C_k(\overline{\rho}) = k$ then $D_{\overline{\rho}}$ is pro-representable. If G satisfies the p-finiteness condition then $D_{\overline{\rho}}$ is representable.*

17. Schlessinger's Criterion

Recall that if $A_1 \xrightarrow{f_1} A \xleftarrow{f_2} A_2$ are morphisms in $\mathcal{C}$ then we can form the fibre product

$$A_1 \times_A A_2 = \{(r_1, r_2) \in R_1 \times R_2 \mid f(x_1) = f(x_2)\}$$

Lemma 17.1. *For $A \in \mathcal{C}$ we have*

$$\mathrm{Hom}(R, A_1 \times_A A_2) = \mathrm{Hom}(R, A_1) \times_{\mathrm{Hom}(R,A)} \mathrm{Hom}(R, A_2)$$

Proof. This is an easy exercise. □

This implies that if $D_{\overline{\rho}}$ is representable then

$$D_{\overline{\rho}}(A_1 \times_A A_2) = D_{\overline{\rho}}(A_1) \times_{D_{\overline{\rho}}(A)} D_{\overline{\rho}}(A_2)$$

for every diagram $A_1 \xrightarrow{f_1} A \xleftarrow{f_2} A_2$ in $\mathcal{C}$. In fact this is essentially the only necessary condition

Theorem 17.2 (Grothendieck)**.** *Let $F : \mathcal{C}^0 \to \underline{\mathrm{Set}}$ be a functor with $F(k) = \{*\}$. Then F is pro-representable if and only if the natural map*

$$F(A_1 \times_A A_2) \to F(A_1) \times_{F(A)} F(A_2) \tag{17.3}$$

is a bijection for every diagram $A_1 \to A \leftarrow A_2$ in $\mathcal{C}^0$. If $F(k[\epsilon])$ is finite then F is representable (i.e the pro-representing object is Noetherian).

Unfortunately, this result is not so useful in general because it is hard to check the fibre product condition for all objects in $\mathcal{C}^0$. Schlessinger's criterion however reduces checking the condition that $F(A_1 \times_A A_2) \to F(A_1) \times_{F(A)} F(A_2)$ is an isomorphism to more simple collection of fibre products.

Definition 17.4. A morphism $A \to B$ in $\mathcal{C}^0$ is *small* if it is surjective and if its kernel is killed by $\mathfrak{m}_A$ and one dimensional over $A/\mathfrak{m}_A = k$.

Theorem 17.5 (Schlessinger's Criterion)**.** *Let $F : \mathcal{C}^0 \to \underline{\text{Set}}$ be a functor with $F(k) = \{*\}$. Then F is representable if and only if the following conditions are satisfied*

(H1) If $A_2 \to A$ is small then (17.3) *is surjective.*
(H2) If $A = k$ and $A_2 = k[\epsilon]$ then (17.3) *is bijective.*
(H3) $F(k[\epsilon])$ is finite.
(H4) If $A_1 = A_2$ and the maps $A_i \to A$ are equal and small then (17.3) *is bijective.*

Exercise 17.6. Use Schlesssinger's criterion to give another proof of the representability of $D^{\square}_{\overline{\rho}}$.

Lets discuss how to use this to this result to prove that $D_{\overline{\rho}}$ is representable when $C_k(\overline{\rho}) = k$. Let $f_i : A_i \to A$ be morphisms in $\mathcal{C}^0$ and define

$$A_3 := A_1 \times_A A_2$$

Since $D^{\square}_{\overline{\rho}}$ is representable we know $D^{\square}_{\overline{\rho}}$ satisfies each of $(H1), \ldots, (H4)$.

Exercise 17.7. Suppose that $f_2 : A_2 \to A$ is surjective. Then

$$1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_2}) \to 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_A)$$

is surjective.

Lemma 17.8. *The map* (17.3) *is surjective whenever $A_2 \to A$ is surjective. In particular, $D_{\overline{\rho}}$ satisfies (H1)*

Proof. By the previous exercise this implies

$$1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_2}) \to 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_A)$$

is surjective. Now suppose $[\rho_i] \in D_{\overline{\rho}}(A_i)$ for $i = 1, 2$ are equivalence classes which become equal in $D_{\overline{\rho}}(A)$. Then there exists $F \in 1 + \mathrm{Mat}(\mathfrak{m}_A)$ such that

$$f_1 \circ \rho_1 = F(f_2 \circ \rho_2)F^{-1}$$

By the above surjectivitiy we can choose $\widetilde{F} \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_2})$ mapping onto F. This means the representations ρ_1 and $\widetilde{F}\rho_2\widetilde{F}^{-1}$ become equal when mapped into $\mathrm{GL}_n(A)$. Hence $(\rho_1, \widetilde{F}\rho_2\widetilde{F}^{-1})$ comes from an element $D^{\square}_{\overline{\rho}}(A_3)$ and so also $([\rho_1], [\rho_2])$. □

We also need to consider when (17.3) is injective. For take $\rho_i \in D^{\square}_{\overline{\rho}}(A_i)$ and set

$$G_i(\rho_i) = \{F \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_i}) \mid F\rho_i(g)F^{-1} = \rho_i(g) \text{ for all } g \in G\}$$

and similarly define $G(\rho)$ for $\rho \in D^{\square}_{\overline{\rho}}(A)$. Note this is contained in $G_i(\rho_i)$ is contained in $C_{A_i}(\rho_i)$.

Lemma 17.9. *Suppose that the induced map*

$$G_2(\rho_2) \to G(f_2 \circ \rho_2)$$

is surjective for every $\rho_2 \in D^{\square}_{\overline{\rho}}(A_2)$. Then (17.3) *is injective.*

Proof. If (17.3) is not injective then there exist $\rho, \rho' \in D^{\square}_{\overline{\rho}}(A_3)$ with images $\rho_i, \rho'_i \in D^{\square}_{\overline{\rho}}(A_i)$ and $F_i \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_i})$ with

$$\rho_i = F_i \rho'_i F_i^{-1}$$

for $i = 1, 2$. Considering the image in $\mathrm{GL}_n(A)$ we get

$$\overline{F}_1(f_1 \circ \rho_1)\overline{F}_1^{-1} = \overline{F}_2(f_2 \circ \rho_2)\overline{F}_2^{-1}$$

where $\overline{F}_i$ is the image of F_i in $\mathrm{Mat}_{n\times n}(A)$. Since $f_1 \circ \rho_1 = f_2 \circ \rho_2$ it follows that $\overline{F}_1\overline{F}_2^{-1} \in G(f_2 \circ \rho)$. By assumption we can lift this to an element $H \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_i})$. Then we can consider

$$H_2 = HF_2 \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_2}), \qquad H_1 = F_1 \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_1})$$

Both these matrices have image $\overline{F}_1$ in $1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_A)$ and so comes from a matrix $H_3 \in 1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_3})$. We have

$$\rho = H_3 \rho' H_3^{-1}$$

since this is true after applying f_1 and f_2. Therefore $[\rho] = [\rho']$. □

Corollary 17.10. *$D_{\overline{\rho}}$ satisfies (H2)*

Proof. We just have to show that if $A_2 = k[\epsilon]$ and $A = k$ then $G_2(\rho_2) \to G(\rho)$ is surjective. But $G(\rho)$ is a single point so this is clear. □

Lemma 17.11. *If G satisfies the p-finiteness hypothesis then $D_{\overline{\rho}}(k[\epsilon])$ is finite.*

Proof. Last time we saw that if G satisfies the p-finiteness hypothesis then $D^{\square}_{\overline{\rho}}(k[\epsilon])$ is finite. Since $D_{\overline{\rho}}(k[\epsilon])$ is surjected on by $D^{\square}_{\overline{\rho}}(k[\epsilon])$ the same is true for $D_{\overline{\rho}}(k[\epsilon])$. □

The last thing to check is (H4). This is where the assumption that $C_k(\overline{\rho}) = k$ comes in.

Lemma 17.12. *If $C_k(\overline{\rho}) = k$ then (H4) is satisfied.*

Proof. We are going to show that $C_A(\rho)$ consists of scalar matrices. For this we induct on the smallest integer such that $\mathfrak{m}_A^n = 0$. If $n = 0$, i.e. if $A = k$, then this is our hypothesis. In general we consider the surjection $A \to B = A/\mathfrak{m}_A^{n-1}$. Note the kernel of this surjection killed by $\mathfrak{m}_A$ and is one dimensional over k. In particular, it is generated by an element say t.

Now suppose $c \in C_A(\rho)$. By induction $C_B(\rho)$ consists of scalar matrices so we can write $c = b + tM$ for b a scalar matrix in A and $M \in \mathrm{Mat}_{n\times n}(k)$. We have

$$(b + tM)\rho(g) = \rho(g)(b + tM), \qquad g \in G$$

Since b is scalar this implies $M\rho(g) = \rho(g)M$ and so $M \in C_k(\overline{\rho}) = k$. We conclude that c is scalar which finishes the induction.

As a consequence we deduce that $G_i(\rho_2)$ also consists of scalar matrices in $1 + \mathrm{Mat}_{n\times n}(\mathfrak{m}_{A_2})$. This shows that

$$G_i(\rho_2) \to G(f_2 \circ \rho_2)$$

is surjective and hence that (17.3) is injective. As we've □

Lecture 11

18. Absolute irreducibility

Let G be a profinite group. In this section we briefly discuss the condition $C_k(\overline{\rho}) = k$ for a continuous representation $\overline{\rho} : G \to \mathrm{GL}_n(k)$ which ensured $D_{\overline{\rho}}$ was representable. Recall

$$C_k(\overline{\rho}) = \{M \in \mathrm{Mat}_{n\times n}(k) \mid M\overline{\rho}(g) = \overline{\rho}(g)M \text{for all } g \in G\}$$

Remark 18.1. If we view $\overline{\rho}$ as giving an action of G on the k-vector space k^n then $C_k(\overline{\rho})$ identifies with $\mathrm{End}_k(\overline{\rho})$ i.e. the set of linear maps $k^n \to k^n$ which commute with the action of G.

Example 18.2. (1) If $\overline{\rho} : G \to \mathrm{GL}_n(k)$ is trivial then $C_k(\overline{\rho}) = \mathrm{Mat}_{n\times n}(k)$.

(2) Suppose $\rho : G \to \mathrm{GL}_2(k)$ is given by

$$\rho(g) = \begin{pmatrix} \chi_1(g) & c(g) \\ 0 & \chi_2(g) \end{pmatrix}$$

If $\chi_1(g) = \chi_2(g)$ then $C_k(\overline{\rho})$ contains all all diagonal matrices so $C_k(\overline{\rho}) \neq k$. If $\chi_1(g) \neq \chi_2(g)$ for some g then $C_k(\overline{\rho})$ is contained in the group of upper triangular matrices.

Definition 18.3. We say that $\overline{\rho}$ is irreducible if there exists no proper non-zero subspace of k^n which is stable under the action of G induced by $\overline{\rho}$. We say that $\overline{\rho}$ is absolutely irreducible there exists no proper non-zero subspace of $\overline{k}^n$ which is stable under the action of G induced by the composite

$$G \xrightarrow{\overline{\rho}} \mathrm{GL}_n(k) \to \mathrm{GL}_n(\overline{k})$$

Example 18.4. Here is an example of a irreducible representation which is not absolutely irreducible. Let G be the cyclic group of order 4 with generator g and assume that k does not contain a square root of -1. Then consider the representation

$$\overline{\rho} : G \to \mathrm{GL}_2(k)$$

given by $\overline{\rho}(g) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. If k^2 contains a non-zero proper subspace then this must be generated by $\alpha e_1 + \beta e_2$. for $\alpha, \beta \in k$ for $e_1, e_2 \in k^2$ the standard basis. Since it is stable there must be $z \in k$ such that

$$\rho(g) \cdot (\alpha e_1 + \beta e_2) = -\beta e_1 + \alpha e_2 = z(\alpha e_1 + \beta e_2)$$

Therefore $z\alpha = -\beta$ and $z\beta = \alpha$. If $\alpha \neq 0$ then $\alpha = z\beta = z(-z\alpha) = -z^2\alpha$ so $z^2 = -1$ which is impossible. Similarly if $\beta \neq 0$. This shows that $\overline{\rho}$ is irreducible. However it is not absolutely irreducible because if $z^2 = -1$ then

$$\rho(g) \cdot (e_1 + ze_2 2) = z(e_1 + ze_2)$$

Lemma 18.5. *If $\overline{\rho} : G \to \mathrm{GL}_n(k)$ is absolutely irreducible then $C_k(\overline{\rho}) = k$.*

Proof. It is enough to show $C_{\overline{k}}(\overline{\rho}) = \overline{k}$. If we view any $M \in C_{\overline{k}}(\overline{\rho})$ as an endomorphism of $\overline{k}^n$ then M must be injective since the kernel if G-stable. Hence M is an isomorphism. It follows that $C_{\overline{k}}(\overline{\rho})$ is a finite dimensional $\overline{k}$-algebra. Any such algebra over an algebraically closed field equals $\overline{k}$ so we are done. □

19. p-finiteness for local Galois groups

Let K be a finite extension of $\mathbb{Q}_p$ and write $G_K = G(\overline{K}/K)$ for $\overline{K}$ an algebraic closure. The goal is to prove

Proposition 19.1. *G_K satisfies the l-finiteness condition for every prime l*

Recall this means that $\mathrm{Hom}(G_0, \mathbb{F}_l)$ is finite for any open subgroup. Since any $G_0 = G_L$ for L/K a finite extension we reduce to showing finiteness of

$$\mathrm{Hom}(G_K, \mathbb{F}_l)$$

Note this is equivalent to showing that K admits only finitely many extensions of degree l. Thus, the following version of Hilbert's theorem 90 is useful:

Theorem 19.2 (Hilbert's Theorem 90). *Let l be a prime and suppose K is a field of characteristic prime to l and containing a l-th root of unity. Then the map*

$$K^\times/(K^\times)^l \to \{\textit{degree } p \textit{ extensions of } K\}$$

sending $[a] \mapsto K(a^{1/l})$ defines a bijection.

Proof of Proposition 19.1. We can prove the finiteness after adjoining an l-th root of unity to K. Therefore, the theorem reduces us to showing that

$$K^\times/(K^\times)^l$$

is a finite group. For this we recall the explicit description of $K^\times$. If we choose a uniformiser $\pi \in K$ then

$$K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$$

We can also write $\mathcal{O}_K^\times = k^\times \times (1 + \mathfrak{m}_K)$. This reduces us to showing that

$$(1 + \mathfrak{m}_K)/(1 + \mathfrak{m}_K)^p$$

is a finite group. For this look at the exact sequence

$$1 \to (1 + \mathfrak{m}_K^n)/(1 + \mathfrak{m}_K)^p \to (1 + \mathfrak{m}_K)/(1 + \mathfrak{m}_K)^p \to Q \to 1$$

Then Q is a quotient of $(1+\mathfrak{m}_K)/(1+\mathfrak{m}_K^n)$ which is a finite group. So we are reduced to showing finiteness of the first term for $n >> 0$. For this recall that the logarithm map

$$1 + x \mapsto x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

defines an isomorphism between $1+\mathfrak{m}_K^n$ and $\mathfrak{m}_K^n$ for n sufficiently large. Thus

$$(1+\mathfrak{m}_K^n)/(1+\mathfrak{m}_K)^p \cong \mathfrak{m}_K^n/p\mathfrak{m}_K^n$$

which is a finite. □

Next we recall the structure of the Galois group G_K. Let k denote the residue field of K (which is a finite field of characteristic p). Recall that for every finite extension l/k there exists a unique extension L/K for which π is a uniformiser of L whenever π is a uniformiser of K. We say such L/K are unramified. This is also equivalent to asking that the map natural map

$$G(L/K) \to G(l/k)$$

for l the residue field of L is an isomorphism. Set

$$K^{\mathrm{ur}} = \bigcup L$$

with the union running over finite unramified subextensions $K \subset L \subset \overline{K}$. Then K^{ur} is normal and there is an exact sequence

$$1 \to G(\overline{K}/K^{\mathrm{ur}}) \to G_K \to G(K^{\mathrm{ur}}/K) \to 1$$

and $G(K^{\mathrm{ur}}/K) \cong G(\overline{k}/k) \cong \widehat{Z}$ where $\overline{k}$ denotes the residue field of $\overline{K}$ which equals an algebraic closure of k. We write

$$I_K = G(\overline{K}/K^{\mathrm{ur}})$$

and call this the inertia subgroup of G_K.

We can also partially describe the structure of I_K. Using Hilbert's Theorem 90 one can prove that

Claim. *Fix a uniformiser $\pi \in K$. Then every degree n extension of K^{ur} for n prime to p can be written as*

$$K_n^{\mathrm{ur}} = K^{\mathrm{ur}}(\pi^{1/n})$$

for $\pi^{1/n}$ an n-th root of π and $G(K_n^{\mathrm{ur}}/K^{\mathrm{ur}}) \cong \mu_n(K^{\mathrm{ur}})$.

As a consequence:

Corollary 19.3. *Set*

$$K^t = \bigcup K_n^{\mathrm{ur}}$$

with the union running over n prime to p. Then there is an isomorphism

$$G(K^t/K^{\mathrm{ur}}) \xrightarrow{\sim} \varprojlim \mu_n(K^{\mathrm{ur}}) \cong \prod_{l \neq p} \mathbb{Z}_l$$

where $\mu_n(K^{\mathrm{ur}})$ denotes the group of n-th roots of unity in K^{ur}. This isomorphism is given by

$$\sigma \mapsto (\sigma(\pi^{1/n})\pi^{-1/n})_n$$

Define $P_K = G(\overline{K}/K^t)$ which we call the wild inertia subgroup. Notice that this is pro-p-group and we have exact sequences

$$1 \to P_K \to I_K \to \prod_{l \neq p} \mathbb{Z}_l \to 1$$

and

$$1 \to \varprojlim \mu_n(K^{\mathrm{ur}}) \to G_K/P_K = G(K^t/K) \to G(K^{\mathrm{ur}}/K) \to 1$$

Any compatible system $(\pi^{1/n})$ of prime to p roots of a uniformiser $\pi \in K$ defines the splitting of this latter exact sequence by sending $\sigma \in G(K^{\mathrm{ur}}/K)$ onto the automorphism of $K^t = \bigcup K^{\mathrm{ur}}(\pi^{1/n})$ which equals σ on K^{ur} and maps $\pi^{1/n}$ onto $\pi^{1/n}$.

Proposition 19.4. *The tame Galois group $G(K^t/K)$ can be topologically generated by two elements σ, τ satisfying the relation*

$$\sigma\tau\sigma^{-1} = \tau^q$$

where q denotes the cardinality of the residue field.

Proof. Choose a compatible sequence $\pi^{1/n}$ as above and suppose that $\sigma \in G(K^t/K)$ is the image under the induced splitting of the element in $G(K^{\mathrm{ur}}/K)$ which acts as $x \mapsto x^q$ on the residue fields. Also, choose a generator in $\varprojlim \mu_n(K^{\mathrm{ur}})$, i.e. a compatible system of primitive n-th roots of unity ζ_n. If n is prime to p then $\sigma(\zeta_n) = \zeta_n^q$ and

$$\tau(\pi^{1/n}) = \zeta_n \pi^{1/n}$$

Therefore $\sigma\tau\sigma^{-1} \in G(K^t/K^{\mathrm{ur}})$ sends

$$\pi^{1/n} \mapsto \pi^{1/n} \mapsto \zeta_n \pi^{1/n} \mapsto \zeta_n^q \pi^{1/n}$$

Since τ^q sends $\pi^{1/n} \mapsto \zeta_n^q \pi^{1/n}$ these automorphisms coincide. □

20. p-finiteness for Global fields

Now suppose that K is a number field with absolute Galois group G_K. It is no longer the case that G_K satisfies the p-finiteness condition. For example, the Kronecker–Weber theorem asserts that

$$G_{\mathbb{Q}}^{\mathrm{ab}} \cong \widehat{\mathbb{Z}}^{\times}$$

and so one can easily compute:

Exercise 20.1. Show that $G_{\mathbb{Q}}$ does not satisfy the p-finiteness condition for any prime p.

However, one can obtain p-finiteness if one restricts the ramification slightly. Suppose L/K is a finite extension of number fields. Recall that for each prime $\mathfrak{p}$ of L lying over $\mathfrak{q}$ in K we say that L/K is unramified at $\mathfrak{p}$ if the extension of local fields $L_{\mathfrak{p}}/K_{\mathfrak{q}}$ is unramified.

Fact 20.2. Let S be any finite set of primes in K. Then there exists a maximal extension K_S of K which is unramified over $\mathbb{Q}$ at any prime not contained in S. This is a Galois extension and we set

$$G_{K,S} = G(K_S/K)$$

which is a quotient of G_K.

Theorem 20.3. *For any finite set $G_{K,S}$ satisfies the p-finiteness hypothesis.*

The proof is more difficult. First one shows

Exercise 20.4. any open normal subgroup of $G_{K,S}$ can be written as $G_{K',S'}$ for some finite extension K' of K and S' some finite set of primes.

Thus the theorem reduces to showing that $\mathrm{Hom}(G_{K,S}, \mathbb{F}_p)$ is finite. This follows from the following important finiteness result:

Theorem 20.5. *(Hermite–Minkowski) Let K be a finite extension of $\mathbb{Q}$ and S a finite set of primes of K. For each integer d there exists finitely many degree d extensions of K which are unramified outside S.*

Lecture 12

21. Example: 1-dimensional local deformation rings

First we will compute deformation rings of one dimensional representations. This will be easy granting results from class field theory:

Theorem 21.1 (Local class field theory)**.** *Let K be a finite extension of $\mathbb{Q}_p$ with maximal abelian extension K^{ab}. There is an injective homomorphism*

$$\Theta : K^\times \to G(K^{\mathrm{ab}}/K)$$

called the Artin map, fitting into a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\cong"] & K^\times \arrow[r, "v"] \arrow[d, "\Theta"] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & G(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \arrow[r] & G(K^{\mathrm{ab}}/K) \arrow[r, "v"] & G(K^{\mathrm{ur}}/K) \arrow[r] & 0
\end{tikzcd}$$

The map Θ induces an isomorphism $\widehat{K}^\times \cong G(K^{\mathrm{ab}}/K)$.

Let $\overline{\rho} : G_K \to \mathrm{GL}_1(\mathbb{F})$ for $\mathbb{F}$ a finite field for K a finite extension of $\mathbb{Q}_p$. Since $\mathrm{GL}_1(R)$ is abelian for every $R \in \mathcal{C}$ (i.e. for every complete local Noetherian ring with residue field $\mathbb{F}$) it follows that every $\rho \in D^{\square}_{\overline{\rho}}(A)$ factors through $G(K^{\mathrm{ab}}/K)$. Therefore

$$D^{\square}_{\overline{\rho}} = D^{\square}_{\overline{\psi}}$$

where $\overline{\psi} : \widehat{K}^\times \to \mathrm{GL}_1(\mathbb{F})$ is obtained by composing $\overline{\rho}$ with the Artin map Θ.

For one-dimensional representations one the following lemma reduces us to the case of deforming the trivial representation

Lemma 21.2. *Suppose $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ and $\overline{\psi} : G \to \mathrm{GL}_1(\mathbb{F})$ are continuous. Set*

$$[\overline{\psi}] : G \to \mathrm{GL}_1(W(\mathbb{F})), [\overline{\psi}](g) = [\overline{\psi}(g)]$$

Then

$$\rho \mapsto \rho \otimes [\overline{\psi}]$$

defines an isomorphism of functors between $D^{\square}_{\overline{\rho}}$ and $D^{\square}_{\overline{\rho}\otimes\overline{\psi}}$. In particular $D^{\square}_{\overline{\rho}}$ is representable if and only if $D_{\overline{\rho}\otimes\overline{\psi}}$ is.

Proof. This is clear. □

Lets consider the case of one dimensional deformations of $G_{\mathbb{Q}_p}$.

Lemma 21.3. *There is an isomorphism*

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$$

of profinite groups. Furthermore, if $1 + p\mathbb{Z}_p$ is viewed as a $\mathbb{Z}_p$-module via

$$\gamma \cdot (1 + X) = \sum_{n\geq 0} \binom{\gamma}{n} X^n$$

then $1 + p\mathbb{Z}_p$ is free of rank one over $\mathbb{Z}_p$ if $p > 2$ and is isomorphic to

$$\{\pm 1\} \times \mathbb{Z}_2$$

for $p = 2$.

Proof. The map is given by $\mathbb{Z} \times \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \to \mathbb{Q}_p^\times$ is given by

$$(n, x, y) \mapsto p^n [x] y$$

For the claim regarding the $\mathbb{Z}_p$-module structure of $1 + p\mathbb{Z}_p$ recall that the logarithm and

$$\log(1 + X) = \sum_{n\geq 0} \frac{(-1)^{n+1} X^n}{n}$$

converges on $1 + p\mathbb{Z}_p$ for $p > 2$ and on $1 + 4\mathbb{Z}_2$. □

Any deformation of the trivial representation factors through the maximal pro-p-quotient of the group. In particular, deformations of the one dimensional trivial representation of $\widehat{\mathbb{Q}_p^\times}$ factor through

- $\widehat{\mathbb{Z}} \times \mathbb{Z}_p$ if $p > 2$ and
- $\widehat{Z} \times \mathbb{Z}_p \times \{\pm 1\}$ is $p = 2$. Therefore

Corollary 21.4. *Let $\overline{\psi} : \widehat{\mathbb{Q}_p^\times} \to \mathrm{GL}_1(\mathbb{F})$ be the trivial character. Then*

(1) *If $p > 2$*

$$R_{\overline{\psi}} = W(\mathbb{F})[[x, y]]$$

is the universal deformation ring of $\overline{\psi}$ and the universal deformation sends

$$\psi^{\mathrm{univ}} : p \mapsto [\overline{\psi}(p)] + x, \quad 1 + p \mapsto [\overline{\psi}(1 + p)] + y$$

(2) *If $p = 2$*

$$R_{\overline{\psi}} = \frac{W(\mathbb{F})[[x,y,z]]}{([\overline{\psi}(-1)] + z)^2 - 1}$$

is the universal deformation ring of $\overline{\psi}$ and the universal deformation is given by

$$\psi^{\mathrm{univ}} : 2 \mapsto [\overline{\psi}(2)] + X, \quad 1 + 4 \mapsto [\overline{\psi}(5)] + Y, \quad -1 \mapsto [\overline{\psi}(-1)] + z)^2$$

Actually, deformation rings of 1-dimensional representations can be described in general using the following construction.

Definition 21.5. Let G be a profinite group. For any ring A define the completed group ring

$$A[[G]] = \varprojlim_{H} A[G/H]$$

with the limit taken over all open normal subgroups $H \subset G$ and $A[G/H]$ equal to the usual group ring, i.e. the free A-module on the elements of G/H with multiplication given by multiplication in G/H.

Lemma 21.6. *Suppose that the ring is profinite. Then $A[[G]]$ is the completion of $R[G]$ for its profinite topology.*

Exercise 21.7. Suppose that A is a complete local Noetherian ring with finite residue field. Then show that continuous homomorphisms $\rho : G \to \mathrm{GL}_n(A)$ are the same thing as continuous A-algebra homomorphisms $A[[G]] \to \mathrm{Mat}_{n\times n}(A)$.

Lemma 21.8. *Suppose that k is a field of characteristic p and G is a finite abelian p-group. Then $k[G]$ is a local ring with maximal ideal generated by $g - 1$ for all $g \in G$.*

Proof. We can write $G = \bigoplus_{i=1}^{r} \mathbb{Z}/p^{a_i}$ for some $a_i \geq 1$. If $g_i \in \mathbb{Z}/p^{a_i}$ are generators then

$$k[G] \cong k[g_1, \dots, g_r]/(X_i^{p^{a_i}} - 1) = k[T_1, \dots, T_r]/(T_i^{p^{a_i}})$$

for $T_i = g_i - 1$ (here we use that $g_i^{p^{a_i}} - 1 = g_i^{p^{a_i}}$ because k has characteristic p. It is easy to see this is local. □

Corollary 21.9. *Suppose that Γ is an abelian pro-p-group. Then $W(\mathbb{F})[[\Gamma]]$ is a complete local ring with residue field $\mathbb{F}$. The maximal ideal is generated by p and $g - 1$ for all $g \in \Gamma$.*

In particular this shows that

$$W(\mathbb{F})[[\mathbb{Z}_p]] \cong W(\mathbb{F})[[T]]$$

via $\gamma - 1 \mapsto T$ for $\gamma \in \mathbb{Z}_p$ any generator.

Proposition 21.10. *Suppose that Γ is a pro-p abelian profinite group and that $\overline{\psi} : \Gamma \to \mathrm{GL}_1(\mathbb{F})$ is continuous. Then the pair $(W(\mathbb{F})[[\Gamma]], \psi^{\mathrm{univ}})$ where*

$$\psi^{\mathrm{univ}} : G \to \mathrm{GL}_1(W(\mathbb{F})[[\Gamma]])$$

is the continuous homomorphism given by $g \mapsto [\overline{\psi}(g)]g$ (here the second g denotes the element in $W(\mathbb{F})[[\Gamma]]$) represents the functor $D^{\square}_{\overline{\psi}}$.

Proof. Using the previous lemma we can assume that $\overline{\psi}$ is the identity. Then any $\Psi \in D^{\square}_{\overline{\psi}}$ corresponds to a homomorphism $G \to 1 + \mathfrak{m}_A$. Extending by $W(\mathbb{F})$-linearity produces a $W(\mathbb{F})$-algebra homomorphism $W(\mathbb{F})[[\Gamma]] \to A$. Conversely, given any $W(\mathbb{F})$-algebra homomorphism $W(\mathbb{F})[[\Gamma]] \to A$ which maps the maximal ideal of $W(\mathbb{F})[[\Gamma]]$ into the maximal ideal of A produces a homomorphism $\Gamma \to W(\mathbb{F})[[\Gamma]] \to 1 + \mathfrak{m}_A$ (note that maximal ideal of $W(\mathbb{F})[[\Gamma]]$ is the kernel of the map $W(\mathbb{F})[[\Gamma]] \to \mathbb{F}$ induced by $g \mapsto 1$ for all $g \in \Gamma$, in particular $\Gamma \subset 1 + \mathfrak{m}_{W(\mathbb{F})[[\Gamma]]}$. □

22. Example: Deformations of some two dimensional p-adic representations

In this example we take $\mathbb{F}$ a field of characteristic $p > 2$ and consider deformations of representations of the form

$$\overline{\rho} : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}), \qquad \overline{\rho}(g) = \begin{pmatrix} 1 & c(g) \\ 0 & 1 \end{pmatrix}$$

for $c(g) : G \to \mathbb{F}$ a 1-cocycle. We've already seen that if $\overline{\rho}$ is trivial then any deformation will factor through the maximal pro-p quotient. In fact:

Exercise 22.1. Note that the image of $\overline{\rho}$ is a p-group. Show this implies that every deformation of $\overline{\rho}$ factors through the maximal pro-p quotient of $G_{\mathbb{Q}_p}$

Let G denote the maximal pro-p-quotient of G. We have already computed the abelianisation of G, namely it was isomorphic $\mathbb{Z}_p \times (1 + p\mathbb{Z}_p)$ (for $p > 2$).

Claim. *Choose $\gamma, \delta \in G$ whose images in G^{ab} respectively identify with $(1, 1+p)$ and $(1, 1)$. Then γ, δ freely generate G.*

Proof. The fact that γ, δ generate G follows from the argument in Lemma 13.8. The fact that γ, δ freely generate is a special case of a more general result we'll see later. □

As a consequence of this claim we deduce that the universal framed deformation ring of $\overline{\rho}$ is

$$R_{\overline{\rho}} = W(\mathbb{F})[[x_{11}, x_{12}, x_{21}, x_{22}, y_{11}, y_{12}, y_{21}, y_{2,2}]]$$

and the universal deformation is ρ^{univ} sends

$$\gamma \mapsto \begin{pmatrix} 1 + x_{11} & x_{12} + [c(\gamma)] \\ x_{21} & x_{22} \end{pmatrix}, \qquad \delta \mapsto \begin{pmatrix} 1 + y_{11} & y_{12} + [c(\delta)] \\ y_{21} & y_{22} \end{pmatrix}$$

23. Example: Deformations of n-dimensional trivial representations

The discussion from the previous section generalises to any finite extension K of $\mathbb{Q}_p$ and any $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ whose image is a p-group (as before $\mathbb{F}$ is assumed to have characteristic p). In particular, when $\overline{\rho}$ is the trivial representation. This requires a description of the maximal pro-p-quotient of G_K which we denote G_K^p.

Using what we know already we can prove:

Lemma 23.1. *Set q equal to the cardinality of $\mu_{p^\infty}(K)$.*

1. *G_K^p is topologically generated by $d+1$ elements if $q = 1$ and $d+2$ is $q > 1$.*
2. *The abelianisation of G_K^p is freely generated as a pro-p-group by $d+2$ elements $g_1, \dots, g_{d+2}$ with the single relation*
$$g_1^q = 1$$

Proof. The argument from Lemma 13.8 implies that any lift to G_K^p of a generating set of $G_K^{p,\mathrm{ab}}$ generates G_K^p. Therefore, (2) implies (1). For (2) note that $G_K^{p,\mathrm{ab}}$ equals the maximal pro-p-quotient of $G_K^{\mathrm{ab}} \cong \widehat{K^\times}$. Hence

$$G_K^{p,\mathrm{ab}} \cong \mathbb{Z}_p \times 1 + \mathfrak{m}_K$$

As when $K = \mathbb{Q}_p$ we can view $1 + \mathfrak{m}_K$ as a $\mathbb{Z}_p$-module. It is finitely generated and its torsion part is $\mu_{p^\infty}(K)$. Hence

$$1 + \mathfrak{m}_K = \mu_{p^\infty}(K) \times \mathbb{Z}_p^r$$

Using that $1 + \mathfrak{m}_K^n \cong \mathfrak{m}_K^n$ via the logarithm for sufficiently large m we see that $1 + \mathfrak{m}_K$ has $\mathbb{Z}_p$-rank $[K : \mathbb{Q}_p]$. Since $\mu_{p^\infty}(K)$ is cyclic of order q this finishes the proof □

Corollary 23.2. *The deformation ring $R_{\overline{\psi}}^{\square}$ for any $\overline{\psi} : G_K \to \mathrm{GL}_1(\mathbb{F})$ can be expressed as*

$$R_{\overline{\psi}}^{\square} = \frac{W(\mathbb{F})[[X_1, \dots, X_{d+2}]]}{(1 + x_1)^q - 1)}$$

The more precise version is:

Theorem 23.3.

1. *(Shafarevich) If $q = 1$ then G_K^p is a free pro-p-group of rank $[K : \mathbb{Q}_p] + 1$.*
2. *(Demuskin) If $q \geq 3$ then G_K^p is the quotient of a free pro-p-group on $d+2$ generators $g_1, \dots, g_{d+2}$ by the relation*
$$g_1^q[g_1, g_2][g_2, g_3] \dots [g_{d+1}, g_{d+2}]$$
where $[g, h] := ghg^{-1}h^{-1}$.

The case $q = 2$ has also been computed by Serre when $[K : \mathbb{Q}_p]$ is odd and Labute when $[K : \mathbb{Q}_p]$ is even.

Corollary 23.4. *Suppose $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ has image a p-group. Then the framed deformation ring $R_{\overline{\rho}}^{\square}$ can be expressed as:*

$$R_{\overline{\rho}}^{\square} = \begin{cases} W(\mathbb{F})[X_1, \dots, X_{d+1}] & \text{if } q = 1 \\ \frac{W(\mathbb{F})[[X_1, \dots, X_{d+2}]]}{((X_1+I)^q[X_1+I, X_2+I] \dots [X_{d+1}+I, X_{d+2}+I] - I)} & \text{if } q > 2 \end{cases}$$

where each X_i is an $n \times n$ matrix of indeterminants.

Finally, we point out an interesting result. Note that for any $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ there is a morphism of functors

$$D_{\overline{\rho}}^{\square} \to D_{\det \overline{\rho}}^{\square}$$

sending a deformation to its determinant (which is viewed as a 1-dimensional representation). This induces a map on deformation rings:

$$R^{\square}_{\det(\overline{\rho})} \to R^{\square}_{\overline{\rho}}$$

If $G = G_K$ for $K/\mathbb{Q}_p$ finite and $\mathbb{F}$ of characteristic p then this map can be written as

$$\frac{W(\mathbb{F})[[X_1, \dots, X_{d+2}]]}{(1+x_1)^q - 1)} \to R^{\square}_{\overline{\rho}}$$

After inverting p and taking Spec the left hand side is a union of q components. In fact a recent theorem (which Paskunas will talk about in the Mittagseminar next week).

Theorem 23.5 (Böckle–Paskunas–Iyengar)**.** *This map induces an bijection*

$$\pi_0(\operatorname{Spec} R^{\square}_{\overline{\rho}}[\frac{1}{p}]) \to \pi_0(\operatorname{Spec} \frac{W(\mathbb{F})[[X_1, \dots, X_{d+2}]]}{(1+x_1)^q - 1)}[\frac{1}{p}])$$

Here π_0 indicates connected components.

Lecture 13

24. H^1 and tangent spaces

For G a profinite group and $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ a continuous homomorphism with $\mathbb{F}$ a finite field recall that the tangent space of the functor $D^{\square}_{\overline{\rho}}$ is

$$D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon]), \qquad \mathbb{F}[\epsilon] = \mathbb{F}[X]/(X^2)$$

We shows that $D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ naturally identified with the group of 1-cocycles $Z^1(G, \mathrm{End}(\overline{\rho}))$ consisting of continuous maps

$$f : G \to \mathrm{Mat}_{n\times n}(\mathbb{F})$$

such that $f(gh) = \overline{\rho}(g)f(h) + f(g)\overline{\rho}(h)$ for all $g, h \in G$. Recall that the bijection was given by the map $Z^1(G, \mathrm{End}(\overline{\rho})) \to D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ which sends

$$f \mapsto \rho_f = (g \mapsto \overline{\rho}(g) + \epsilon f(g))$$

where $\overline{\rho}(g) + \epsilon f(g)$ is viewed as an element in $\mathrm{GL}_n(\mathbb{F}[\epsilon])$.

Proposition 24.1. *Let $B^1(G, \mathrm{End}(\overline{\rho})) \subset Z^1(G, \mathrm{End}(\overline{\rho}))$ be the subspace consisting of functions $f : G \to \mathrm{Mat}_{n\times n}(\mathbb{F})$ with*

$$f(g) = \overline{\rho}(g)X - X\overline{\rho}(g)$$

for some $X \in \mathrm{Mat}_{n\times n}(\mathbb{F})$. Then the map $Z^1(G, \overline{\rho}) \to D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ induces a bijection

$$\frac{Z^1(G, \mathrm{End}(\overline{\rho}))}{B^1(G, \mathrm{End}(\overline{\rho}))} \xrightarrow{\sim} D_{\overline{\rho}}(\mathbb{F}[\epsilon])$$

Proof. Consider two 1-cocycles f, f' and $g \in G$. An easy computation shows that there exists $1 + \epsilon Y \in 1 + \epsilon \operatorname{Mat}_{n\times n}(\mathbb{F})$ so that

$$(1 + \epsilon Y)\,(\overline{\rho}(g) + \epsilon f(g))\,(1 - \epsilon Y) = \overline{\rho}(g) + \epsilon f'(g)$$

if and only if

$$f(g) + Y\overline{\rho}(g) - \overline{\rho}(g)Y = f'(g)$$

Therefore $f - f' \in B^1(G, \overline{\rho})$ if and only if the images of f and f' in $D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ are equivalent (i.e. represent the same element in $D_{\overline{\rho}}(\mathbb{F}[\epsilon])$). □

25. Cohomology of discrete G-modules

Let G be a profinite group and A a G-module, i.e. an abelian group A equipped with an additive action of G.

Definition 25.1. A G-module is discrete if the action map $G \times A \to A$ is continuous when A is given the discrete topology.

Exercise 25.2. Show that a G-module A is a discrete G-module if and only if the stabliser in G of any element in A is an open subgroup if and only if $A = \bigcup A^U$ where U runs over open subgroups of G and A^U denotes the subgroup of A fixed by all elements in U.

Example 25.3. Let $\rho : G \to \mathrm{GL}_n(R)$ be continuous with $R \in \mathcal{C}^0$ (i.e. R is an Artinian local ring with finite residue field). Then ρ makes R^n into a discrete G-module. This is because the $\mathfrak{m}_R$-adic topology on R is the discrete topology (as $\mathfrak{m}_R^n = 0$ for $n >> 0$).

Warning 25.4. However, if $R \in \mathcal{C}$ (i.e. R is a complete local Noetherian local ring with finite residue field) then R^n with the G-action induced by ρ need not make R^n into a discrete module. This is not such a problem for us because we've seen $D^{\square}_{\overline{\rho}}$ is entirely determined by its values on $\mathcal{C}^0$.

Now we show that our construction of $H^1(G, \overline{\rho})$ is the special case of a more general construction. For any discrete G-module A set $C^n(G, A)$ equal to the abelian group of continuous maps $G^n \to A$. Then one can define a coboundary map

$$d : C^n(G, A) \to C^{n+1}(G, A)$$

by the formula

$$\begin{aligned}(df)(g_1, \dots, g_{n+1}) = {} & g_1 f(g_2, \dots, g_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\ & + (-1)^{n+1} f(g_1, \dots, g_n)\end{aligned}$$

This produces a complete

$$\dots \to C^n(G, A) \xrightarrow{d} C^{n+1}(G, A) \xrightarrow{d} C^{n+2}(G, A) \to \dots$$

and one defines $H^n(G,A)$ as the cohomology of this complex. In other words, one defines

$$H^n(G,A) := \frac{\ker(C^n(G,A) \xrightarrow{d} C^{n+1}(G,A))}{\operatorname{im}(C^{n-1}(G,A) \xrightarrow{d} C^n(G,A))}$$

For small n the $H^n(G,A)$ can be described explicity:

(1) For $n < 0$ one has $H^n(G,A) = 0$.

(2) One has $H^0(G,A) = \ker(C^0(G,A) \xrightarrow{d} C^1(G,A))$. If $a \in C^0(G,A) = A$ then $d(a)(g) = g(a) - a$. Therefore $a \in H^0(G,A)$ if and only if $g(a) = a$ for all $g \in G$. Hence $H^0(G,A) = A^G$.

(3) For $n = 1$ notice that any $f \in \ker(C^1(G,A) \to C^2(G,A))$ is a function $f : G \to A$ such that

$$(df)(g_1,g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0$$

for all $g_1, g_2 \in G$. In other words, $f(g_1 g_2) = g_1 f(g_2) + f(g_1)$. We also see that $f \in \operatorname{Im}(C^0(G,A) \to C^1(G,A))$ means that $f(g) = ga - a$ for some $a \in A$. Hence

$$H^1(G,A) = \frac{\{f : G \to A \mid f(gh) = f(g) + gf(h)\}}{\{f : G \to A \mid f(g)ga - a \text{ for some } a \in A\}}$$

Lemma 25.5. *Let $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ be continuous and write $\mathrm{End}(\overline{\rho})$ for the discrete G-module with underlying abelian group $\mathrm{Mat}_{n\times n}(\mathbb{F})$ and G-action given by conjugation with $\overline{\rho}(g)$. Then*

$$\ker(C^1(G,\mathrm{End}(\overline{\rho}) \xrightarrow{d} C^2(G,\mathrm{End}(\overline{\rho}))) = Z^1(G,\mathrm{End}(\overline{\rho}))$$

and

$$H^1(G,\mathrm{End}(\overline{\rho})) = \frac{Z^1(G,\overline{\rho})}{B^1(G,\overline{\rho})} = D_{\overline{\rho}}(\mathbb{F}[\epsilon])$$

Proof. The first equality is given by the map

$$f \mapsto (g \mapsto f(g)\overline{\rho}(g))$$

Since this identifies

$$\operatorname{im}(C^0(G,\mathrm{End}(\overline{\rho})) \xrightarrow{d} C^1(G,\mathrm{End}(\overline{\rho}))) = B^1(G,\mathrm{End}(\overline{\rho}))$$

the first equality induces the second. □

26. Interpretation of H^2 in terms of deformation theory

We've just seen the relevance of H^1 with regards our deformation functor $D^{\square}_{\overline{\rho}}$. The second cohomology groups are also important. To explain this consider the following setup. Let

$$A_1 \to A$$

be a small morphism in $\mathcal{C}^0$. Recall this means that it is surjective and the kernel is killed by $\mathfrak{m}_{A_1}$ and is one-dimensional as an $\mathbb{F} = A_1/\mathfrak{m}_{A_1}$-vector space. This means that the kernel is generated by a single element say q. Then one can wonder whether the map

$$D^{\square}_{\overline{\rho}}(A_1) \to D^{\square}_{\overline{\rho}}(A)$$

is surjective. In other words, can deformations to A be lifted to A_1. We'll see later that if this is always the case then the corresponding deformation ring will be as nice as possible (a power series ring). There is a cohomological critera for liftings to exist:

Construction 26.1. Fix $\rho \in D^{\square}_{\overline{\rho}}(A)$ and fix a set-theoretic mapping

$$\rho_1 : G \to \mathrm{GL}_n(A_1)$$

which equals ρ after composing with $\mathrm{GL}_n(A_1) \to \mathrm{GL}_n(A)$ and define $c : G^2 \to \mathrm{Mat}_{n\times n}(\mathbb{F})$ by

$$c(g_1, g_2) = \rho_1(g_1 g_2)\rho_1(g_2)^{-1}\rho_1(g_1)^{-1} - 1 \in \mathrm{Mat}_{n\times n}(\ker(A_1 \to A)) = \mathrm{Mat}_{n\times n}(\mathbb{F})$$

Exercise 26.2. Show that $c(g_1, g_2) \in \ker(C^2(G, \mathrm{End}(\overline{\rho})) \xrightarrow{d} C^3(G, \mathrm{End}(\overline{\rho})))$.

Suppose ρ_1' is another choice of lifting of ρ. Then

$$\rho_1' - \rho_1 = F \in C^1(G, \mathrm{Mat}_{n\times n}(\ker A_1 \to A)) = C^1(G, \mathrm{End}(\overline{\rho}))$$

Since the kernel of $A_1 \to A$ is square-zero, one has

$$(\rho_1(x) + F(x))^{-1} = (\rho_1(x)^{-1} - \rho_1(x)^{-1}F(x)\rho_1(x)^{-1}) = (\rho_1(x)^{-1} - \overline{\rho}(x)^{-1}F(x))$$

Therefore

$$\begin{aligned} c'(x,y) &= (\rho_1(xy) + F(xy))(\rho_1(y)^{-1} - \overline{\rho}(y)^{-1}F(y)\overline{\rho}(y)^{-1})(\rho_1(x)^{-1} - \overline{\rho}(x)^{-1}F(x)\overline{\rho}(x)^{-1}) \\ &= c(x,y) + F(xy)\overline{\rho}(y)^{-1}\overline{\rho}(x)^{-1} - \overline{\rho}(x)F(y)\overline{\rho}(y)^{-1}\overline{\rho}(x)^{-1} - F(x)\overline{\rho}(x)^{-1} \\ &= c(x,y) + G(xy) - \overline{\rho}(x)G(y)\overline{\rho}(x)^{-1} + G(x) \\ &= c(x,y) + (dG)(x,y) \end{aligned}$$

for $G(x) := F(x)\overline{\rho}(x)^{-1}$. As a consequence this construction produces a well defined element of $H^2(G, \mathrm{End}(\overline{\rho}))$ which we denote by $c(\rho)$.

Proposition 26.3. *The deformation ρ is contained in the image of*

$$D^{\square}_{\overline{\rho}}(A) \to D^{\square}_{\overline{\rho}}(A)$$

if and only if $c(\overline{\rho}) = 0$ in $H^2(G, \mathrm{End}(\overline{\rho}))$. In particular, if $H^2(G, \mathrm{End}(\overline{\rho})) = 0$ then $D^{\square}_{\overline{\rho}}(A) \to D^{\square}_{\overline{\rho}}(A)$ is surjective for every small map $A_1 \to A$.

Proof. If ρ is in the image then we can choose ρ_1 as in the definition so that ρ_1 is a homomorphism. Thus $c = 0$ and so $c(\rho) = 0$. Conversely, if $c(\rho) = 0$ we can choose ρ_1 so that the associated function $c = 0$. Therefore ρ_1 is a homomorphism. □

27. General tools to compute group cohomology

Long exact sequences. Suppose that $0 \to A \to B \to C \to 0$ is a G-equivaraiant exact sequence of discrete A-modules. Then one obtains an exact sequences

$$0 \to C^n(G,A) \to C^n(G,B) \to C^n(G,C) \to 0$$

and hence an exact sequence of complexes

$$0 \to C^\bullet(G,A) \to C^\bullet(G,B) \to C^\bullet(G,C) \to 0$$

(this is the definition of such an exact sequence).

Lemma 27.1. *There exists an associated long exact sequence of cohomology groups*

$$\ldots \to H^i(G,A) \to H^i(G,B) \to H^i(G,C) \xrightarrow{\delta} H^{i+1}(G,A) \to \ldots$$

Proof. This follows by applying the snake lemma to the following diagram

$$\begin{tikzcd}
 & C^i(G,A)/\operatorname{im} d_A^{i-1} \arrow[r] \arrow[d] & C^i(G,B)/\operatorname{im} d_B^{i-1} \arrow[r] \arrow[d] & C^i(G,C)/\operatorname{im} d_C^{i-1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker d_A^i \arrow[r] & \ker d_B^i \arrow[r] & \ker d_C^i &
\end{tikzcd}$$

□

Sometimes this general formalism is enough. For example if you know the $H^i(G,A)$ and $H^i(G,C)$ all vanish then this exact sequence gives vanishing of the middle terms. But sometimes you really need to understand what this map δ really is: here is the simplest example

Example 27.2. The map $\delta : H^0(G,C) \to H^1(G,A)$ can be defined as follows. Take $x \in C^G = H^0(G,C)$ and choose an element $y \in B$ mapping onto x. Then

$$\delta(x)(g) = gy - y$$

Change of group. Let G and G' be two profinite groups, and let $f : G \to G'$ be a homomorphism. Suppose that A and A' are respectively discrete G and G'-modules and that $h : A \to A'$ is a continuous map of abelian groups such that

$$h(gx) = f(g)h(x)$$

for $g \in G, x \in A$. Then one obtains a map of complexes

$$C^\bullet(G',A') \to C^\bullet(G,A)$$

and hence maps on cohomology

$$H^i(G',A') \to H^i(G,A)$$

This construction is particularly useful when we consider the inclusion of a closed subgroup $H \subset G$ and when we take $A = A'$. This gives the restriction homomorphism

$$\operatorname{Res} : H^i(G,A) \to H^i(H,A)$$

(on functions it is just given by restriction). The following is particularly useful:

Proposition 27.3. *Suppose that $H \subset G$ is open and that the index $(G : H) = n$. Then the kernel of* Res *is killed by n. In particular, if A is a p-group and $(G : H)$ is prime to p then the restriction map is injective.*

Corollary 27.4. *Suppose that G has order prime to p and the G-module A is a p-group. Then $H^i(G, A) = 0$ for $i \geq 1$.*

Proof. Applying the previous proposition with $H = \{1\}$ shows that $H^i(G, A)$ injects into $H^i(\{1\}, A)$. Since

$$H^i(\{1\}, A) = \begin{cases} A & \text{if } i = 0 \\ 0 & \text{if } i > 0 \end{cases}$$

it follows that $H^i(G, A) = 0$ for $i \geq 1$. □

Another useful tool for computing cohomology is the restriction–inflation exact sequence. Let $N \subset G$ be a closed normal subgroup and suppose A is a discrete G-module.

Claim. *There is an action of G/N on $H^i(N, A)$. For $i = 1$ (which is all we need) this is induced by the action on 1-cocycles action*

$$g \cdot f(n) = gf(g^{-1}ng)$$

Exercise 27.5. Check this defines a G/N-action.

Then the inflation–restriction exact sequence says that the sequence

$$0 \to H^1(G/N, A^N) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(G, A)^{G/N}$$

is exact. The first map is inflation (coming by the change of group functoriality) and the second is the restriction map.

Remark 27.6. In fact this sequence extends can be continued further:

$$0 \to H^1(G/N, A^N) \to H^1(G, A) \to H^1(G, A)^{G/N} \to H^2(G/N, A^N) \to H^2(G, A)$$

Shapiro's Lemma. One can define induced discrete G-modules which recovers the usual notion of induced representations for finite groups. For this, let $H \subset G$ be a closed subgroup and suppose that A is a discrete H-module. Set $\mathrm{Ind}_H^G(A)$ equal to the set of continuous maps

$$a^* : G \to A$$

satisfying $a^*(hx) = ha^*(x)$ for $h \in H, x \in G$. We can view $\mathrm{Ind}_H^G(A)$ as a discrete G-module via the G-action

$$(g \cdot a^*)(x) = a^*(xg)$$

Evaluating at $1 \in G$ produces a map $\mathrm{Ind}_H^G(A) \to A$ which is compatible with the inclusion $H \to G$. Therefore, we obtain homomorphisms

$$H^i(G, \mathrm{Ind}_H^G(A)) \to H^i(H, A)$$

Proposition 27.7 (Shapiro's lemma)**.** *These are isomorphisms*

Sketch. The proof is easy if one interprets the cohomology $H^i(G,-)$ as the derived functors of the fixed point function $A \mapsto A^G$. Indeed, $A \mapsto \mathrm{Ind}_H^G(A)$ is exact and Frobenius reciprocity implies that it sends injective objects to injective objects. □

Exercise 27.8. Prove Shapiro's lemma directly using the cocycle description for $i = 0, 1$.

Lecture 14

28. Theorems for computing cohomology of local Galois groups

We begin with the cohomological version of Hilbert's theorem 90:

Proposition 28.1. *Here K is any field. Then for any Galois extension K'/K one has $H^1(G(K'/K), K'^{\times}) = 0$ and $H^q(G(K'/K), K') = 0$ for $q \geq 1$.*

As a corollary we find:

Corollary 28.2. *Let n be an integer prime to the characteristic of K and let $\mu_n(K)$ denote the group of n-th roots of unity in K. Then $H^1(G_K, \mu_n(K)) = K^{\times}/(K^{\times})^n$.*

Proof. From the exact sequence of G_K-modules $1 \to \mu_n(K) \to \overline{K}^{\times} \xrightarrow{x \mapsto x^n}\!\!\!\!\to \overline{K} \to 1$ we obtain an exact sequence

$$H^0(G_K, \overline{K}^{\times}) \to H^0(G_K, \overline{K}^{\times}) \to H^1(G_K, \mu_n(K)) \to H^1(G_K, \overline{K}^{\times})$$

The first map is the n-th power map $K^{\times} \to K^{\times}$ so we obtain an inclusion $K^{\times}/(K^{\times})^n \to H^1(G_K, \mu_n(K))$. Since $H^1(G_K, \overline{K}^{\times}) = 0$ this inclusion is a surjective. □

Definition 28.3. For a profinite group G and a prime l set $\mathrm{cd}_l(G)$ equal to the l-cohomological dimension of G. This is the smallest (possibly infinite) integer for which the p-primary part of $H^i(G, A) = 0$ is zero whenever $i \geq \mathrm{cd}_l(G)$. One sets $\mathrm{cd}(G)$ equal to the supremum of the $\mathrm{cd}_l(G)$ as l runs over all primes.

From now on we assume the field K is a finite extension of $\mathbb{Q}_p$.

Theorem 28.4. *For $G = G_K$ one has $\mathrm{cd}(G) = 2$.*

Therefore the only relevant cohomology groups in this case are given by H^0, H^1 and H^2. The next theorem of Tate reduces calculations of H^2 to those of H^0.

Theorem 28.5. *Assume that A is a finite G_K-module. Set μ equal to the G_K-module obtained as the union of $\mu_n(\overline{K})$ for all n. Then there is a perfect pairing*

$$H^i(G_K, A) \times H^{2-i}(G_K, \mathrm{Hom}(A, \mu)) \to \mathbb{Q}/\mathbb{Z}$$

We are most interested in the case where A is a finite dimensional $\mathbb{F}_l$-vector space for some prime l. Specialising the theorem in this situation gives:

Corollary 28.6. *Suppose that A is a finite dimensional $\mathbb{F}_l$-vector space. Then there are isomorphisms*

$$H^0(G_K, A) \cong H^2(G_K, \mathrm{Hom}(A, \mu_l))$$

as groups. Similarly

$$H^1(G_K, A) \cong H^1(G_K, \mathrm{Hom}(A, \mu_l))$$

Here we write μ_l for the G_K-module $\mu_l(\overline{K})$.

Proof. The theorem gives an isomorphism

$$H^0(G_K, A) \cong \mathrm{Hom}_{\mathbb{Z}}(H^2(G_K, \mathrm{Hom}(A, \mu)), \mathbb{Q}/\mathbb{Z})$$

Since A is an $\mathbb{F}_l$-vector space we have $\mathrm{Hom}(A, \mu) = \mathrm{Hom}(A, \mu_l(\overline{K}))$. Also $H^2(G_K, \mathrm{Hom}(A, \mu_l)$ is an $\mathbb{F}_l$-vector space so we can replace the $\mathbb{Q}/\mathbb{Z}$ by its l-torsion subgroup which is $[\frac{1}{l}]\mathbb{Z}/\mathbb{Z} \cong \mathbb{F}_l$. Therefore

$$H^0(G_K, A) \cong \mathrm{Hom}_{\mathbb{F}_l}(H^2(G_K, \mathrm{Hom}(A, \mu_l)), \mathbb{F}_l)$$

□

We can make this even more explicit. A G_K-module A with $A = \mathbb{F}^n$ for $\mathbb{F}$ a finite field of characteristic l is the same thing as a continuous representation $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$. If we choose an identification $\mu_l \cong \mathbb{F}_l$ by fixing a primitive l-th root of unity ζ_l in $\overline{K}$ then the action of G_K on μ_l is given by the l-cyclotomic character:

$$\chi_{\mathrm{cyc},l} : G_K \to \mathbb{F}_l^\times$$

defined by the identity $g(\zeta_l) = \zeta_l^{\chi_{\mathrm{cyc},l}(g)}$ for $g \in G_K$. Therefore, the G_K-module $\mathrm{Hom}(A, \mu_l)$ corresponds to the continuous representation $\overline{\rho}^\vee \otimes \chi_{\mathrm{cyc},l} : G_K \to \mathrm{GL}_n(\mathbb{F})$ given by

$$\overline{\rho}^\vee \otimes \chi_{\mathrm{cyc},l}(g) = \overline{\rho}(g^{-1})^{\mathrm{t}} \chi_{\mathrm{cyc},l}(g)$$

Here X^t denotes the transpose of a matrix X.

Example 28.7.
- We have $H^2(G_K, \chi_{\mathrm{cyc},l}) = H^0(G_K, \mathbb{F}_l) = \mathbb{F}_l$.
- We also have $H^1(G_K, \mathbb{F}_l) = H^1(G_K, \mu_l) = K^\times/(K^\times)^l$.

The last important result for computing cohomology of p-adic fields is Tate's Euler characteristic formula. For any finite G_K-module A set

$$\chi(A) = \frac{h^0(A)h^2(A)}{h^1(A)}$$

where $h^i(A)$ denotes the cardinality of the finite group $H^i(G_K, A)$. Note that if A is an $\mathbb{F}_l$-module then the Euler characteristic contains the same information as the alternating sum

$$\dim_{\mathbb{F}_l} H^0(G_K, A) - \dim_{\mathbb{F}_l} H^1(G_K, A) + \dim_{\mathbb{F}_l} H^2(G_K, A)$$

which is the more familiar definition of the Euler characteristic.

Exercise 28.8. Show that if $0 \to A \to B \to C \to 0$ is an exact sequence of finite G_K-modules then $\chi(B) = \chi(A)\chi(C)$.

We first give an easier special case of the main theorem:

Proposition 28.9. *If the order of A is prime to p then $\chi(A) = 1$.*

Proof. Let k denote the residue field of K. Our proof will use two facts:

- The first is that the inflation–restriction exact sequence from last time can be extended to a 7-term! long exact sequence:
$$\begin{aligned}0 \to H^1(G/N, A^N) \to H^1(G, A) \to H^1(N, A)^{G/N} \to H^2(G/N, A^N)\\ \to \ker\big(H^2(G, A) \to H^2(N, A)\big) \to H^1(G/N, H^1(N, A))\\ \to \ker\big(H^3(G/N, A^N) \to H^3(G, A)\big)\end{aligned}$$
- $H^i(I_K, A) = 0$ and $H^i(G_k, A) = 0$ for $i \geq 2$.

Let k denote the residue field of K and recall the inertia subgroup $I_K \subset G_K$. Then one sees directly from the definitions that

$$H^0(G_K, A) = H^0(I_K, A)^{G_k}$$

The inflation-restriction long exact sequence gives that

$$H^2(G_K, A) = H^1(G_k, H^1(I_K, A))$$

because $H^2(I_K, A) = H^3(G_k, A^{I_K}) = 0$. We also get

$$0 \to H^1(G_k, A^{I_K}) \to H^1(G_K, A) \to H^1(I_K, A)^{G_k} \to 0$$

because $H^2(G_k, A) = 0$. Therefore

$$\chi(A) = \frac{\operatorname{Card}(H^0(I_K, A)^{G_k}) \operatorname{Card}(H^1(G_k, H^1(I_K, A)))}{\operatorname{Card}(H^1(G_k, A^{I_K})) \operatorname{Card}(H^1(I_K, A)^{G_k})}$$

The result therefore follows from the computation that for any finite $\mathbb{Z}$-module A both $H^0(\widehat{\mathbb{Z}}, A)$ and $H^1(\widehat{\mathbb{Z}}, A)$ have the same cardinality. □

The general result which computes χ is:

Theorem 28.10. *Let A be a finite G_K-module of cardinality a. Then*

$$\chi(A) = ||a||$$

where $||a||$ denotes the absolute value on K normalised so that $||p|| = p^{[K:\mathbb{Q}_p]}$.

When A is an $\mathbb{F}_l$-vector space then we can reformulate this in terms of the alternating sum of the dimensions of the cohomology groups. When $l \neq p$ it just says that this alternating sum is zero. When $l = p$ it shows that

$$\dim H^0(G_K, A) - \dim H^1(G_K, A) + \dim H^2(G_K, A) = [K : \mathbb{Q}_p] \dim A$$

We'll see later that these alternating sums are related to the dimension of our deformation rings.

29. Examples: mod p representations of a p-adic field

Continue to assume that K is a finite extension of $\mathbb{Q}_p$ and consider a continuous representation of $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ with $\mathbb{F}$ a finite field. We've seen that computing the cohomology of $\mathrm{End}(\overline{\rho})$ is useful for understanding the corresponding deformation ring $R_{\overline{\rho}}$. Here we'll discuss some examples of these computations.

The cases where $\mathbb{F}$ has characteristic $l \neq p$ and $l = p$ behave very differently. Here we'll try to understand the case where $l = p$. This is based on the following key lemma:

Lemma 29.1. *Let G be a p-group acting on a finite dimensional $\mathbb{F}_p$-vector space A. Then $H^0(G, A) = 0$ if and only if $A = 0$.*

Proof. Assume $A \neq 0$ and $A \smallsetminus \{0\}$ has no fixed points. Then every G-orbit in A contains > 1 element. By the orbit-stabiliser theorem the cardinality of every G-orbit divides that of G. Thus, every G-orbit in $A \smallsetminus \{0\}$ has order divisible by p. But this is a contradiction since it implies

$$\mathrm{Card}(A \smallsetminus \{0\}) \equiv 0 \text{ modulo } p$$

□

Corollary 29.2. *Suppose that $\mathbb{F}$ has characteristic p and $\overline{\rho}$ is irreducible. Then $\overline{\rho}$ factors through the tame Galois group $G(K^t/K) = G_K/P_K$.*

Proof. Since P_K is a pro-p-group the previous lemma implies that $\overline{\rho}$ contains a non-zero vector v fixed by P_K. Since $\overline{\rho}$ is irreducible it is generated as a $\mathbb{F}[G_K]$-module by v. Therefore P_K acts trivially on the whole of $\overline{\rho}$. □

This has the following important consequence. Recall that if $H \subset G$ is a closed subgroup and A is a discrete H-module then we defined the induction $\mathrm{Ind}_H^G A$.

Proposition 29.3. *Assume that $\mathbb{F} = \overline{\mathbb{F}}_p$ and that $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ is irreducible. Then there exists an unramified extension L/K such that and a 1-dimensional representation $\chi : G_L \to \mathrm{GL}_1(\mathbb{F})$ such that*

$$\overline{\rho} \cong \mathrm{Ind}_L^K \chi := \mathrm{Ind}_{G_L}^{G_K} \chi$$

Proof. Set $V = \overline{\rho}$ viewed as a G-module for $G = G(K^t/K)$ and write I^t for the tame inertia subgroup, i.e. the kernel of $G \to G_k$. Then $I^t \cong \prod_{l \neq p} \mathbb{Z}_l$ and so is abelian of order prime to p. Therefore $V|_{I^t}$ is semi-simple (note this uses that $\mathbb{F} = \overline{\mathbb{F}}_p$) as an I^t-module and so we can write

$$V|_{I^t}$$

as a direct sum of $\chi : I^t \to \mathbb{F}^\times$. If $\gamma \in G$ and χ is such a character then we can define $\chi^{(\gamma)}$ by setting

$$\chi^{(\gamma)}(g) = \chi(\gamma^{-1} g \gamma)$$

Note this character only depends upon the image of γ in G_k. If I^t acts on $v \in V$ via χ then it acts on γv by $\chi^{(\gamma)}$. This shows that the group G_k acts on the set of characters appearing in $V|_{I_t}$. Fix such a χ and set $H \subset G$ be the normal subgroup corresponding to the stabiliser of χ in G_k equal to its stabiliser. The orbit–stabiliser theorem says that

$$[G:H] \leq \dim_{\mathbb{F}} V$$

On the other hand, Frobenius recirocity (i.e. Shapiro's lemma for H^0) produces a non-zero map $V|_H \to \operatorname{Ind}_{I^t}^H \chi$.

Lemma 29.4. *The character χ extends to a character $\widetilde{\chi} : H \to \mathbb{F}^\times$.*

Proof. Suppose L/K is the unramified extension corresponding to H. Then $H = G(L^t/L)$ and we've seen that H is generated by two elements σ, τ with $\tau \in I^t$ and $\sigma\tau\sigma^{-1} = \tau^{\operatorname{Card} l}$. The fact that H is the stabiliser of χ implies that $\chi(\tau^q) = \chi(\tau)$. Therefore we can define an extension of χ be mapping $\sigma \mapsto 1$. □

This lemma implies that $\operatorname{Ind}_{I^t}^H \chi = \widetilde{\chi} \otimes \operatorname{Ind}_{I^t}^H 1$ (by the projection formula) where 1 is the trivial character. Note that this is a representation of H/I^t. Since $\operatorname{Ind}_{I^t}^H 1$ is a discrete submodule we can find a finite dimensional stable submodule $R \subset \operatorname{Ind}_{I^t}^H 1$ so that $V|_H \to \operatorname{Ind}_{I^t}^H \chi$ factors through $\widetilde{\chi} \otimes R$. Since H/I^t is abelian R admits a composition series $0 = R_n \subset R_{n-1} \subset \ldots \subset R_1 \subset R_0 = R$ with each R_i/R_{i+1} one dimensional. Choose i maximal so that $V|_H \to \operatorname{Ind}_{I^t}^H \chi$ factors through $\chi \otimes R_i$. Then the induced map

$$V|_H \to \chi \otimes R_i \to \chi \otimes R_i/R_{i+1}$$

is non-zero. Therefore Frobenius reciprocity produces a non-zero map

$$V \to \operatorname{Ind}_H^G(\chi \otimes R_i/R_{i+1})$$

Since V is irreducible this is injective so $\dim V \leq \dim \operatorname{Ind}_H^G(\chi \otimes R_i/R_{i+1})$. Since $\chi \otimes R_i/R_{i+1}$ is one dimensional this dimension is $[G:H]$. Since we know $[G:H] \geq \dim V$ this is an equality and the map is an isomorphism. □

Lecture 15

30. Mod p Galois representations (continued)

We contained the discussion from the last part of the previous lecture. Recall that K was a finite extension of $\mathbb{Q}_p$. We say that if $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ was a continuous irreducible representation with $\mathbb{F} = \overline{\mathbb{F}}_p$ then

$$\overline{\rho} \cong \operatorname{Ind}_L^K \chi := \operatorname{Ind}_{G_L}^{G_K} \chi$$

for $\chi : G_L \to \mathbb{F}^\times$ a continuous character and L/K an unramified extension. Therefore, if we can understand such characters then we can understand all irreducible mod p representations.

To do this note any such χ factors through the tame Galois group $G(L^t/L)$ which can be topologically generated by two elements σ, τ satisfying $\sigma\tau\sigma^{-1} = \tau^q$ for $q = \operatorname{Card}(l)$ (l the residue field of L). Therefore, any such character is determined by two elements in $\mathbb{F}^\times$

- $\chi(\sigma)$ (this can be any element)
- $\chi(\tau)$ which must satisfy $\chi(\tau) = \chi(\tau)^q$. Thus $\chi(\tau) \in \mathbb{F}_q^\times \subset \mathbb{F}^\times$.

Conversely, any two such elements produces a continuos character. In particular, if we choose a generator of $\mathbb{F}_q^\times$ then we can define a *fundamental character*

$$\omega_L : G_L \to \mathbb{F}^\times$$

by setting $\omega(\sigma) = 1$ and $\omega(\tau)$ equal to the chosen generator of $\mathbb{F}_q^\times$. Of course this description involves many choices; but there is a more natural description of these fundamental characters.

Construction 30.1. Fix a uniformiser $\pi \in K$ and an embedding $\tau : l \hookrightarrow \mathbb{F}$. Then we can define a continuous character $\omega_L : G_L \to \mathbb{F}^\times$ by composing

$$g \mapsto \text{ the image in } l^\times \text{ of } \frac{g(\pi^{1/(q-1)})}{\pi^{1/(q-1)}}$$

with τ.

Exercise 30.2. Prove that this character is a fundamental character and that its restriction to I_L is independent of the choice of π.

Proposition 30.3. *Fix a fundamental character ω_L. Then every continuous character $\chi : G_L \to \mathbb{F}^\times$ can be written uniquely as*

$$\psi \otimes \omega_L^{\sum_{i=0}^{f-1} a_i p^i}$$

for $0 \le a_i \le p-1$ and f defined by $q = p^f$.

Proof. We've just seen that such χ are determined by where they send σ and τ. Where they send σ determines the unramified character ψ and they must send τ onto an element of $\mathbb{F}_q^\times = (\mathbb{Z}/q\mathbb{Z})^\times$. Any such element can be written uniquely as

$$\sum_{i=0}^{f-1} a_i p^i$$

for $0 \le a_i \le p-1$ which gives the result. □

Example 30.4. We've seen that every irreducible representation has the form $\mathrm{Ind}_L^K \chi$ for χ one dimensional. However, not every such induction will be irreducible (if χ is the trivial character this is obvious because the induced representation is the regular representation of G_K/G_L). In fact, Mackey's criterion implies that $\mathrm{Ind}_L^K \chi$ is irreducible if and only if χ cannot be extended to a character of $G_M \to \mathbb{F}^\times$ for $K \subset M \subsetneq L$. With notation as in the proposition this occurs if and only if

$$\sum_{i=0}^{f-1} a_i p^i \notin \mathbb{F}_{p^{f-1}}$$

Exercise 30.5. Show that restriction of the cyclotomic character to G_L can be written as

$$\chi_{\mathrm{cyc}} = \psi \otimes \omega_L^{\sum_{i=0}^{f-1} p^i}$$

for some unramified ψ.

Example 30.6 (Classification of two dimensional mod p representations of $G_{\mathbb{Q}_p}$)**.** Suppose $\overline{\rho} : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F})$ is continuous. Then, either:

- $\overline{\rho} \cong \psi \otimes \mathrm{Ind}_{\mathbb{Q}_{p^2}}^{\mathbb{Q}_p}(\omega_{\mathbb{Q}_{p^2}}^a)$ for $0 \le a < p^2 - 1$ and $p+1$ not dividing a. Here $\mathbb{Q}_{p^2}$ is the degree 2 unramified extension of $\mathbb{Q}_p$.
- $$\overline{\rho} \cong \psi \otimes \begin{pmatrix} \chi_{\mathrm{cyc}}^a & * \\ 0 & \chi_{\mathrm{cyc}}^b \end{pmatrix}$$
  for $0 \le a, b < p-1$.

Proposition 30.7. *Suppose that $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ is continuous and that K does not contain a p-th root of unity. Then*

$$H^2(G_K, \mathrm{End}(\overline{\rho})) = 0$$

except possibly if

$$\overline{\rho} \cong \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

for characters χ_i satisfying $\chi_1\chi_2^{-1} = \chi_{\mathrm{cyc}}^{-1}$.

Proof. Using Tate duality we know $H^2(G_K, \mathrm{End}(\overline{\rho})) = H^0(G_K, \mathrm{End}(\overline{\rho})^\vee \otimes \chi_{\mathrm{cyc}})$. Recall the $\vee$ denotes the $\mathbb{F}$-linear dual. We can write

$$\mathrm{End}(\overline{\rho})^\vee = \mathrm{End}(\overline{\rho}^\vee)$$

and $\mathrm{End}(\overline{\rho}^\vee) \otimes \chi_{\mathrm{cyc}} = \mathrm{Hom}(\overline{\rho}^\vee, \overline{\rho}^\vee \otimes \chi_{\mathrm{cyc}})$. Therefore, $H^2(G_K, \mathrm{End}(\overline{\rho}))$ is zero if and only if there exist no non-zero G_K-equivariant homomorphisms

$$\overline{\rho}^\vee \to \overline{\rho}^\vee \otimes \chi_{\mathrm{cyc}}$$

The assumption that K contains no p-th root of unity implies χ_{cyc} is non-trivial. In particular, if $\overline{\rho}$ is irreducible (which implies $\overline{\rho}^\vee$ is irreducible) then no such map can exist. If $\overline{\rho}$ is reducible then

$$\overline{\rho}^\vee = \begin{pmatrix} \chi_2^{-1} & * \\ 0 & \chi_1^{-1} \end{pmatrix}$$

If $* = 0$ then any such G_K-equivariant map must induce either an isomorphism $\chi_2^{-1} \cong \chi_1^{-1} \otimes \chi_{\mathrm{cyc}}$ or an isomorphism $\chi_1^{-1} \cong \chi_2^{-1} \otimes \chi_{\mathrm{cyc}}$. Swapping χ_1 and χ_2 if necessary this gives the lemma. For the non-split case, any G-equivariant map must have a non-zero kernel (otherwise it would be an isomorphism and this is impossible since χ_{cyc} is non-trivial). If $\chi_1 \neq \chi_2$ then this kernel must be the only G-stable subspace corresponding to χ_2^{-1}. In this case, any G-equivariant map would induce an isomorphism $\chi_1^{-1} \cong \chi_2^{-1} \otimes \chi_{\mathrm{cyc}}$. If $\chi_1 = \chi_2$ then the case $* = 0$ shows there can be no map after semi-simplifying, and therefore no map before semi-simplifying. □

31. Obstruction Theory

Now we return to the general setup with G a profinite group and $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$. Here we also return to the case where $\mathbb{F}$ is just a finite field. We saw in Lecture 13 that if $H^2(G, \overline{\rho}) = 0$ then for any surjective morphism $A \to B$ in $\mathcal{C}^0$ (recall this is the category of Artin local rings with residue field $\mathbb{F}$) the corresponding map

$$D^{\square}_{\overline{\rho}}(A) \to D^{\square}_{\overline{\rho}}(B)$$

was surjective. With the definition below this means that the morphism of functors

$$D^{\square}_{\overline{\rho}} \to \mathrm{pt}$$

(where pt is the functor sending any ring A onto the set consisting of one element) is formally smooth.

Definition 31.1. Let $F \to G$ be a morphism of set valued functors on $\mathcal{C}^0$. We say this morphism is formally smooth if for the every surjective morphism $A \to B$ in $\mathcal{C}^0$ the map

$$F(A) \to F(B) \times_{G(B)} G(A)$$

is surjective.

We know that $D^{\square}_{\overline{\rho}} \cong \mathrm{Hom}(R^{\square}_{\overline{\rho}}, -)$, and we can also write $\mathrm{pt} = \mathrm{Hom}(W(\mathbb{F}), -)$ since every object in $A \in \mathcal{C}^0$ admits a unique morphism $W(\mathbb{F}) \to A$ in $\mathcal{C}$ (recall this means that the map of rings induces the identity on residue fields).

Definition 31.2. Let $R \to S$ be a morphism in $\mathcal{C}$. We say that $R \to S$ is formally smooth if the morphism of functors

$$\mathrm{Hom}(S, -) \to \mathrm{Hom}(R, -)$$

on $\mathcal{C}^0$ is formally smooth. Equivalently, for every commutative diagram

$$\begin{tikzcd} S \arrow[r] & B \\ R \arrow[u] \arrow[r] & A \arrow[u] \end{tikzcd}$$

with $A \to B$ surjective there exists a morphism $S \to A$ making

$$\begin{tikzcd} S \arrow[r] \arrow[dr] & B \\ R \arrow[u] \arrow[r] & A \arrow[u] \end{tikzcd}$$

commute.

Corollary 31.3. *Assume that $R_{\overline{\rho}}$ is representable (e.g. if G satisfies the p-finiteness hypothesis). If $H^2(G, \mathrm{End}(\overline{\rho})) = 0$ then the morphism $W(\mathbb{F}) \to R^{\square}_{\overline{\rho}}$ is formally smooth.*

To motivate the name formal smoothness we recall what it means for a map of rings $R \to S$ to be smooth. The easiest definition to write down is that for every $f \in R$ mapping into an invertible element in S one can write

$$S = R_f[x_1, \dots, x_n]/(f_1, \dots, f_c)$$

so that

$$g = \det\left(\frac{\partial f_i}{\partial x_j}\right)$$

maps onto an invertible element in S. Note there are two issues with this definition. Firstly, it requires $R \to S$ to be of finite presentation (which may not be the case for maps like $\mathbb{Z}_p \to \mathbb{Z}_p[[X]]$). Secondly, this definition in terms of partial derivatives is often not very useful in practice. However one can show that (a version of) formal smoothness (for general rings) and finite presentation is equivalent to being smooth. So really formal smoothness is the better definition.

Proposition 31.4. *Suppose that $R \to S$ is a formally smooth morphism in $\mathcal{C}$. Then*

$$S \cong R[[X_1, \dots, X_n]]$$

for some $n \geq 0$.

Proof. If $S \cong R[[X_1, \dots, X_n]]$ then this is clear. Choose generators $x_1, \dots, x_n \in S$ whose images generate the $S/\mathfrak{m}_S = \mathbb{F}$-vector space $\mathfrak{m}_S/(\mathfrak{m}_S^2 + \mathfrak{m}_R S)$. Set $T = R[[X_1, \dots, X_n]]$. Then we have a commutative diagram

$$\begin{tikzcd}
S \arrow[r, "u_1"] & T/(\mathfrak{m}_T^2 + \mathfrak{m}_R T) \\
R \arrow[u] \arrow[r] & T/\mathfrak{m}_T^2 \arrow[u]
\end{tikzcd}$$

where u_1 sends x_i onto the class of X_i. By formal smoothness we can lift u_1 to a morphism $u_2 : S \to T/\mathfrak{m}_T^2$. Iterating the procedure using the diagram

$$\begin{tikzcd}
S \arrow[r, "u_n"] & T/\mathfrak{m}_T^n \\
R \arrow[u] \arrow[r] & T/\mathfrak{m}_T^{n+1} \arrow[u]
\end{tikzcd}$$

and formal smoothness to lift u_n to $u_{n+1} : S \to T/\mathfrak{m}_T^{n+1}$ we obtain a morphism $u : S \to \varprojlim_n T/\mathfrak{m}_T^n \cong T$. We have to show this is an isomorphism.

By a result from Lecture 5, for surjectivity it suffices to show that the induced map $\mathbb{F} \to T/\mathfrak{m}_S T$ is surjective and that T is $\mathfrak{m}_S T$-adically complete. In other words, we have to show that $\mathfrak{m}_S T = \mathfrak{m}_T$. We know $\mathfrak{m}_S T \subset \mathfrak{m}_T$ because u is a morphism in $\mathcal{C}$. For the opposite inclusion we note that

$$X_i \equiv u(x_i) \text{ modulo } \mathfrak{m}_T^2 + \mathfrak{m}_R T$$

Since $\mathfrak{m}_R T$ is contained in the image of u we can actually write

$$X_i \equiv u(x_{i,1}) \text{ modulo } \mathfrak{m}_T^2$$

for some $x_{i,1} \in \mathfrak{m}_S$. Since $\mathfrak{m}_T^2$ is generated over R by the X_iXj's we can write

$$X_i \equiv u(x_{i,2}) \text{ modulo } \mathfrak{m}_T^3$$

Inducting and using completeness gives $X_i \in \mathfrak{m}_S T$.

For injectivity choose $y_i \in S$ so that $u(y_i) = X_i$ (we can do this by surjectivity). Then $u : S \to T$ has an R-linear section $T \to S$ sending X_i onto y_i. This finishes the proof. □

Corollary 31.5. *If $R_{\overline{\rho}}^{\square}$ represents $D_{\overline{\rho}}^{\square}$ and $H^2(G, \mathrm{End}(\overline{\rho})) = 0$ then*

$$R_{\overline{\rho}}^{\square} \cong W(\mathbb{F})[[X_1, \ldots, X_n]]$$

Also $n = \dim_{\mathbb{F}} D_{\overline{\rho}}^{\square}(\mathbb{F}[\epsilon])$.

Here is another application of formal smoothness.

Lemma 31.6. *Suppose that $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ has $D_{\overline{\rho}}$ representable by $R_{\overline{\rho}}$. Then*

$$R_{\overline{\rho}}^{\square} \cong R_{\overline{\rho}}[[X_1, \ldots, X_{n^2 - \dim H^0(G, \mathrm{End}(\overline{\rho}))}]]$$

Proof. First, lets show $R_{\overline{\rho}}^{\square} \cong R_{\overline{\rho}}[[X_1, \ldots, X_m]]$ for some m. By the above it suffices to show that the morphism of functors

$$D_{\overline{\rho}}^{\square} \to D_{\overline{\rho}}$$

is formally smooth. Let $A \to B$ be a surjective morphism in $\mathcal{C}^0$. We have to show

$$D_{\overline{\rho}}^{\square}(A) \to D_{\overline{\rho}}(A) \times_{D_{\overline{\rho}}(B)} D_{\overline{\rho}}^{\square}(B)$$

is surjective. An element in the target corresponds to $\rho_A : G \to \mathrm{GL}_n(A)$ and $\rho_B : G \to \mathrm{GL}_n(B)$ so that if $\rho_{A,B}$ is the composite of ρ_A with $\mathrm{GL}_n(A) \to \mathrm{GL}_n(B)$ then $Y\rho_{A,B}Y{-}1 = \rho_B$ for some $Y \in 1 + \mathrm{Mat}(\mathfrak{m}_B)$. Since $A \to B$ is surjective so is $\mathfrak{m}_A \to \mathfrak{m}_B$. Therefore we can choose $\widetilde{Y} \in 1 + \mathrm{Mat}(\mathfrak{m}_A)$. Set $\rho = Y\rho_A Y^{-1} \in D_{\overline{\rho}}^{\square}(A)$. Then ρ is mapped onto $([\rho_A], \rho_B)$.

To show that $m = n^2$ we examine the proof of Proposition 31.4. If $\mathfrak{m}$ and $\mathfrak{m}^{\square}$ are the maximal ideals of $R_{\overline{\rho}}$ and $R_{\overline{\rho}}^{\square}$ respectively then the proof shows that

$$m = \dim_{\mathbb{F}} \mathfrak{m}^{\square}/(\mathfrak{m}^{\square,2} + \mathfrak{m}R_{\overline{\rho}}^{\square})$$

Thus it is dimension of the cokernel of the map $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}^{\square}/\mathfrak{m}^{\square,2}$. Recall $\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, \mathbb{F}) = D_{\overline{\rho}}(k[\epsilon])$ and likewise for framed deformations. Therefore m is also the kernel of the map

$$D_{\overline{\rho}}^{\square}(\mathbb{F}[\epsilon]) \to D_{\overline{\rho}}(\square)$$

Recall also that this can be described as the quotient

$$Z^1(G, \mathrm{End}(\overline{\rho})) \to H^1(G, \mathrm{End}(\overline{\rho}))$$

whose kernel is precisely the set of coboundaries $B^1(G, \mathrm{End}(\overline{\rho}))$, i.e. the set of $f : G \to \mathrm{Mat}(\mathbb{F})$ with $f(g) = \overline{\rho}(g)X - X\overline{\rho}(g)$. Thus, we have an exact sequence

$$0 \to H^0(G, \mathrm{End}(\overline{\rho})) \to \mathrm{Mat}_{n \times n}(\mathbb{F} \to B^1(G, \mathrm{End}(\overline{\rho})) \to 0$$

and so $m = n^2 - \dim H^0(G, \mathrm{End}(\overline{\rho}))$. □

Note, we only know $D_{\overline{\rho}}$ is representable when $H^0(G, \mathrm{End}(\overline{\rho})) = 0$ so in basically all cases one has $R^{\square}_{\overline{\rho}} \cong R_{\overline{\rho}}[[X_1, \dots, X_{n^2}]]$.

Lecture 16

32. Krull dimension and regular local rings

Definition 32.1. Let R be a Noetherian ring. We say that a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$$

in R has length n and define the Krull dimension $\mathrm{Krull}(R)$ of R to be the supremum of the lengths of all such chains of prime ideals.

Example 32.2. The Krull dimension of $W(\mathbb{F})[[X_1, \dots, X_n]] = n + 1$. One example of a maximal length chain of ideals is

$$(0) \subset (p) \subset (p, X_1) \subset \dots \subset (p, X_1, \dots, X_n)$$

Example 32.3. If $\mathrm{Krull}(R) = 0$ then every prime ideal is maximal. Thus, dimension zero rings are the same as Artinian rings.

We are most interested in the case where R is a complete local ring with finite residue field $\mathbb{F}$. We have previously seen that if $x_1, \dots, x_n \in \mathfrak{m}_R$ have images generating $\mathfrak{m}_R/\mathfrak{m}_R^2$ then the map

$$W(\mathbb{F})[[X_1, \dots, X_n]] \to R$$

sending $X_i \mapsto x_i$ is surjective and induces an isomorphism

$$(X_1, \dots, X_n, p)/(X_1, \dots, X_n, p)^2 \cong \mathfrak{m}_R/(\mathfrak{m}_R^2)$$

of $n + 1$-dimensional $\mathbb{F}$-vector spaces. Directly from the definition we see that

$$\mathrm{Krull}(R) \leq \mathrm{Krull}(W(\mathbb{F})[[X_1, \dots, X_n]]) = n + 1$$

Thus

$$\mathrm{Krull}(R) \leq \dim_{\mathbb{F}} \mathrm{Hom}(\mathfrak{m}_R/(\mathfrak{m}_R^2), \mathbb{F})$$

Example 32.4. Here are some examples where you don't have equality:

- Let $R = \mathbb{F}[[x, y]]/(xy)$. Then $\mathrm{Krull}(R) = 1$ (because R is completed local ring at the intersection of two lines) but $\mathfrak{m}_R/\mathfrak{m}_R$ is generated over $\mathbb{F}$ by the images of x and y, and hence is two dimensional.
- Let $R = \mathbb{F}[x]/x^n$. Then $\mathrm{Krull}(R) = 0$ because R is Artinian and so every prime ideal is maximal. However $\mathfrak{m}_R/\mathfrak{m}_R^2$ is generated by the image of x and is one-dimensional.

The more general assertion is that

Theorem 32.5. *Let R be a ring and suppose that $x_1, \dots, x_c \in R$ and that P is minimal amongst all prime ideals in R containing $x_1, \dots, x_c$. Then the maximal length of a chain of prime ideals*

$$\mathfrak{p}_0 \subsetneq \dots \subset \mathfrak{p}_n = P$$

is $\leq c$.

This also gives (for more general rings R) that $\operatorname{Krull}(R)$ is less than the dimension $\mathfrak{m}_R/\mathfrak{m}_R^2$ because if $x_1, \ldots, x_n$ have images generating $\mathfrak{m}_R/\mathfrak{m}_R^2$ then there can be no prime ideal $(x_1, \ldots, x_n) \subset P \subsetneq \mathfrak{m}_R$.

Definition 32.6. Let R be a Noetherian local ring. Then R is a regular local ring if the inequality $\operatorname{Krull}(R) \leq \dim_{\mathbb{F}} \mathfrak{m}_R/\mathfrak{m}_R^2$ is an equality.

Proposition 32.7. *Let $R \to S$ be a morphism in $\mathcal{C}$. Then the following are equivalent*

(1) S is a flat R-algebra and $R/\mathfrak{m}_S R$ is a regular local $\mathbb{F}$-algebra.
(2) $R \to S$ is formally smooth.

Proof. See Tag 07NQ on the stacks project. □

Remark 32.8. We point out that in this theorem it is significant that the residue field of R and S is perfect.

In particular this gives another way to deduce that a complete local Noetherian ring R with residue field $\mathbb{F}$ is isomorphic to $W(\mathbb{F})[[X_1, \ldots, X_n]]$. One has to show that R is $W(\mathbb{F})$-flat (since $W(\mathbb{F})$ is a discrete valuation ring this is the same as proving it is p-torsionfree) and that R/pR is a regular local ring, i.e. that

$$\operatorname{Krull}(R/pR) = \dim_{\mathbb{F}}(\mathfrak{m}_R, p)/(\mathfrak{m}_R, p)^2$$

If R is p-torsion free then $\operatorname{Krull}(R/pR) = \operatorname{Krull} R - 1$. In particular, this gives:

Corollary 32.9. *Let $R_{\overline{\rho}}^{\square}$ represent $D_{\overline{\rho}}^{\square}$. Suppose that*

$$n = \dim_{\mathbb{F}} D_{\overline{\rho}}^{\square}(\mathbb{F}[\epsilon]) = \operatorname{Krull} R - 1$$

Then $R_{\overline{\rho}}^{\square} \cong W(\mathbb{F})[[X_1, \ldots, X_n]]$.

Exercise 32.10. Prove the claim that if R is p-torsionfree then $\operatorname{Krull}(R/pR) = \operatorname{Krull}(R) - 1$.

33. Lower bounds on dimensions of deformation rings

We've seen that the dimension of $H^1(G_K, \operatorname{End}(\overline{\rho}))$ or $Z^1(G_K, \operatorname{End}(\overline{\rho}))$ gives upper bounds on the dimensions of $R_{\overline{\rho}}$ and $R_{\overline{\rho}}^{\square}$. The goal here is to give the following lower bound:

Proposition 33.1. *Assume $\overline{\rho} : G \to \operatorname{GL}_d(\mathbb{F})$ is continuous and G satisfies the p-finiteness hypothesis.*

$$\operatorname{Krull}(R_{\overline{\rho}}^{\square}/pR_{\overline{\rho}}^{\square}) \geq d^2 - \dim H^0(G, \operatorname{End}(\overline{\rho})) + \dim H^1(G, \operatorname{End}(\overline{\rho})) - \dim H^2(G, \operatorname{End}(\overline{\rho}))$$

Proof. Set $R = R_{\overline{\rho}}^{\square}$.

First recall that the kernel of $Z^1(G, \operatorname{End}(\overline{\rho})) \to H^1(G, \operatorname{End}(\overline{\rho}))$ consists of coboundaries $B^1(G, \operatorname{End}(\overline{\rho}))$ and there is an exact sequence

$$0 \to H^0(G, \operatorname{End}(\overline{\rho})) \to \operatorname{End}(\overline{\rho}) \to B^1(G, \operatorname{End}(\overline{\rho})) \to 0$$

Thus

$$n := \dim \mathfrak{m}_R/(\mathfrak{m}_R^2 + pR) = d^2 - \dim H^0(G, \operatorname{End}(\overline{\rho})) + \dim H^1(G, \operatorname{End}(\overline{\rho}))$$

Therefore we can find an exact sequence

$$0 \to J \to F = \mathbb{F}[[X_1, \dots, X_n]] \to \overline{R} = R/pR \to 0$$

which induces an isomorphism $\mathfrak{m}_{\overline{R}}/\mathfrak{m}_{\overline{R}}^2 = \mathfrak{m}_F/\mathfrak{m}_F^2$.

Lemma 33.2. $\mathrm{Krull}(\overline{R}) \geq n - \dim \mathrm{Hom}(J/\mathfrak{m}_{\mathbb{F}}J, \mathbb{F})$

Proof. This follows by applying Theorem **??** with to elements $x_1, \dots, x_n \in J$ whose images form a basis of $J/\mathfrak{m}_F J$. Then there can be no prime ideals $(x_1, \dots, x_n) \subset P \subsetneq Q \subset J$ and so the maximal length of a chain of primes contained in J is at most $\dim \mathrm{Hom}(J/\mathfrak{m}_{\mathbb{F}}J, \mathbb{F})$.

Since $n = \mathrm{Krull}(F)$ equals the sum of $\mathrm{Krull}\, \overline{R}$ and the maximal length of a chain of primes in J we have the claimed inequality (this uses that F satisfies a condition called being catenary). □

We have to prove that $\dim \mathrm{Hom}(J/\mathfrak{m}_{\mathbb{F}}J, \mathbb{F}) \leq \dim H^2(G, \mathrm{End}\, \overline{\rho})$. To do this set $\rho_p : G \to \mathrm{GL}_n(\overline{R})$ equal to $\rho^{\mathrm{univ}} \otimes_R \overline{R}$. Thus, ρ_p is universal amongst all deformations to $A \in \mathcal{C}$ with $pA = 0$. A slight variant of the construction from before of obstruction classes produces

$$c(\rho_p) : \left[(g,h) \mapsto \widetilde{\rho}_p(gh)\widetilde{\rho}_p(h)^{-1}\widetilde{\rho}_p(g)^{-1} - 1\right] \in H^2(G, \mathrm{End}(\overline{\rho}) \otimes J/\mathfrak{m}_F J)$$

for some set-theoretic lift $\widetilde{\rho}_p : G \to \mathrm{GL}_n(F/\mathfrak{m}_F J)$ of ρ_p. Just as before, this class is independent of the choice of $\widetilde{\rho}_p$. Then we obtain a map

$$\mathrm{Hom}(J/\mathfrak{m}_F J, \mathbb{F}) \to H^2(G, \mathrm{End}(\overline{\rho}))$$

which sends f onto the image of $c(\rho_p)$ under the induced homomorphism

$$H^2(G, \mathrm{End}(\overline{\rho}) \otimes J/\mathfrak{m}_F J) \to H^2(G, \mathrm{End}(\overline{\rho}))$$

Concretely

$$f \mapsto [(g,h) \mapsto f\left(\widetilde{\rho}_p(gh)\widetilde{\rho}_p(h)^{-1}\widetilde{\rho}_p(g)^{-1} - 1\right)]$$

If we can show this map is injective then we will be done.

Suppose $f \in \mathrm{Hom}(J/\mathfrak{m}_F J, \mathbb{F})$ is non-zero. To any such f we can produce a quotient A of $F/\mathfrak{m}_F J$ by setting $A = F/(\mathfrak{m}_F J + \ker f)$. Then we have an exact sequence

$$0 \to I \to A \to \overline{R} \to 0$$

where $I \cong \mathrm{im}\, f = \mathbb{F}$. In particular, this is a small extension and the image of f in $H^2(G, \mathrm{End}(\overline{\rho}))$ is precisely the obstruction class associated to this small extension and $\overline{\rho}_p$. If f is mapped onto zero then this obstruction class vanishes and so there exists a lift of ρ_p to $\rho_A \in D^{\square}_{\overline{\rho}}(A)$. By universality, such a ρ_A corresponds to homomorphism $R \to A$ and so a homomorphism $\overline{R} \to A$ (since $pA = 0$). This homomorphism produces a splitting of the exact sequence

$$0 \to I \to A \to \overline{R} \to 0$$

However, since $A \to \overline{R}$ is an isomorphism on tangent spaces this is impossible (it would imply that $I = 0$). We conclude that the kernel of $\mathrm{Hom}(J/\mathfrak{m}_F J, \mathbb{F}) \to H^2(G, \mathrm{End}(\overline{\rho}))$ is zero which finishes the proof. □

Corollary 33.3. *Suppose that* $H^0(G, \mathrm{End}(\overline{\rho})) = \mathbb{F}$*. Then*

$$H^1(G, \mathrm{End}(\overline{\rho})) \geq \mathrm{Krull}(R_{\overline{\rho}}/pR_{\overline{\rho}}) \geq \dim H^1(G, \mathrm{End}(\overline{\rho})) - \dim H^2(G, \mathrm{End}(\overline{\rho}))$$

Combining these results with Tate's Euler characteristic formula gives:

Proposition 33.4. *Suppose* $G = G_K$ *for* $K/\mathbb{Q}_p$ *a finite extension and suppose* $\mathbb{F}$ *has characteristic* l*. Then*

(1) If $l \neq p$ *then*

$$\mathrm{Krull}(R^{\square}_{\overline{\rho}}/pR^{\square}_{\overline{\rho}}) \geq d^2$$

and if $H^0(G_K, \mathrm{End}(\overline{\rho})) = \mathbb{F}$ *then*

$$\mathrm{Krull}(R_{\overline{\rho}}/pR_{\overline{\rho}}) \geq 0$$

(2) If $l = p$ *then*

$$\mathrm{Krull}(R^{\square}_{\overline{\rho}}/pR^{\square}_{\overline{\rho}}) \geq d^2 + [K : \mathbb{Q}_p]d^2$$

and if $H^0(G_K, \mathrm{End}(\overline{\rho})) = \mathbb{F}$ *then*

$$\mathrm{Krull}(R_{\overline{\rho}}/pR_{\overline{\rho}}) \geq [K : \mathbb{Q}_p]d^2$$

There is also the following conjecture:

Conjecture 33.5. *Suppose* $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ *is absolutely irreducible. Then*

$$\mathrm{Krull}(R_{\overline{\rho}}/pR_{\overline{\rho}}) = \dim H^1(G, \mathrm{End}(\overline{\rho})) - \dim H^2(G, \mathrm{End}(\overline{\rho}))$$

34. Relation to Leopoldt's conjecture

We'll finish by explaining how the previous conjecture can be thought of as a generalisation of Leopoldt's conjecture. More precisely, we'll explain how this conjecture is equivalent to Leopoldt's conjecture when G is the Galois group of a number field and $\overline{\rho}$ is 1-dimensional.

First suppose that $G = G_{K,S}$ where K is a finite extension of $\mathbb{Q}$ and S is a finite set of places of K. Assume that S contains all the infinite places of K and all places above $p = \mathrm{char}\,\mathbb{F}$. Set $S_\infty \subset S$ the set of infinite places. In this case one has a global version of the Euler characteristic formula: for any discrete G-module M

$$\frac{\mathrm{Card}\, H^0(G, M)\, \mathrm{Card}\, H^2(G, M)}{\mathrm{Card}\, H^1(G, M)} = \frac{1}{(\mathrm{Card}\, M)^{[K:\mathbb{Q}]}} \prod_{v \in S_\infty} \mathrm{Card}\, H^0(G_{K_v}, M)$$

Note here K_v is either $\mathbb{R}$ or $\mathbb{C}$ depending on whether v is a real or complex place. Thus G_{K_v} is has at most two elements. Taking $M = \mathrm{End}(\overline{\rho})$ gives

$$\begin{aligned} &-\dim H^0(G, \mathrm{End}(\overline{\rho})) + \dim H^1(G, \mathrm{End}(\overline{\rho})) - \dim H^2(G, \mathrm{End}(\overline{\rho})) \\ &\quad = \sum_{v \in S_\infty} \dim H^0(G_{K_v}, \mathrm{End}(\overline{\rho})) - [K : \mathbb{Q}]d^2 \end{aligned}$$

Now suppose that $\overline{\rho}$ is the trivial character. Then combining the global Euler characteristic formula with the lower bound from the previous section implies that

$$\begin{aligned}\mathrm{Krull}(R_{\overline{\rho}}/pR_{\overline{\rho}}) &\geq 1 + [K:\mathbb{Q}] - \sum_{v \in S_\infty} \dim \mathrm{Hom}(G_{K_v}, \mathbb{F}) \\ &= 1 + \mathrm{Card}(\{\text{number of complex places of } K\})\end{aligned}$$

Here we use that $[K:\mathbb{Q}]$ equals the sum of the number of real places and twice the number of complex places. On the other hand, we know that $R_{\overline{\rho}} = W(\mathbb{F})[[G_{K,S}^{p,\mathrm{ab}}]]$ for $G_{K,S}^{p,\mathrm{ab}}$ the maximal pro-p quotient of $G_{K,S}^{\mathrm{ab}}$. Therefore, the dimension of $R_{\overline{\rho}}$ equals the rank of $G_{K,S}^{p,\mathrm{ab}}$ as a $\mathbb{Z}_p$-module and so

$$\mathrm{Krull}(R_{\overline{\rho}}) = \dim \mathrm{Hom}(G_{K,S}^{p,\mathrm{ab}}, \mathbb{F}_p)$$

One formulation of Leopoltd's conjecture is

Conjecture 34.1. *The $\mathbb{Z}_p$-rank of $G_{K,S}^{p,\mathrm{ab}}$ equals* 1+ *the number of complex places of K.*

In particular, the conjecture regarding the dimension of $R_{\overline{\rho}}$ is equivalent to Leopoltd's conjecture in this particular case.

Lecture 17

35. Closed loci in deformation rings

For many applications one is not interested in all deformations but only those which satisfy certain specific conditions. If these specific conditions are chosen well then one is able to construct a closed subspace of $\mathrm{Spec}\, R_{\overline{\rho}}^{\square}$ or $\mathrm{Spec}\, R_{\overline{\rho}}$ which classifies deformations for which these conditions hold.

Definition 35.1. Fix a profinite group G and let $\mathcal{Q}$ be a property of continuous representations $\rho : G \to \mathrm{GL}_n(A)$ for $A \in \mathcal{C}^0$. We say that $\mathcal{Q}$ is a *deformation problem* inside $D_{\overline{\rho}}^{\square}$ if the following conditions are satisfied:

1. $\overline{\rho}$ has property $\mathcal{Q}$.
2. If $A \to B$ is a morphism in $\mathcal{C}^0$ and $\rho \in D_{\overline{\rho}}^{\square}(A)$ has property $\mathcal{Q}$ then also the image of ρ in $D_{\overline{\rho}}^{\square}(B)$ has $\mathcal{Q}$.
3. Let

$$\begin{tikzcd} & A \times_C B \arrow[dl] \arrow[dr] & \\ A \arrow[dr] & & B \arrow[dl] \\ & C & \end{tikzcd}$$

be a fibre product in $\mathcal{C}^0$ and let $\rho \in D_{\overline{\rho}}^{\square}(A \times_C B)$ with images $\rho_A \in D_{\overline{\rho}}^{\square}(A)$ and $\rho_B \in D_{\overline{\rho}}^{\square}(B)$. Then ρ has property $\mathcal{Q}$ if and only if ρ_A and ρ_B have property $\mathcal{Q}$.

Note that condition (2) implies that the rule

$$D^{\Box}_{\overline{\rho},\mathcal{Q}} : \mathcal{C}^0 \to \underline{\mathrm{Set}}$$

given by

$$A \mapsto \{\rho \in D^{\Box}_{\overline{\rho}}(A) \text{ with property } \mathcal{Q}\}$$

is a subfunctor of $D^{\Box}_{\overline{\rho}}$.

Definition 35.2. Let $D : \mathcal{C}^0 \to \underline{\mathrm{Set}}$ be a subfunctor of $D^{\Box}_{\overline{\rho}}$. We say that D is a closed subfunctor if D is representable by an object in $\mathcal{C}$.

The following lemma indicates why we call such subfunctors closed:

Lemma 35.3. *If $D \subset D^{\Box}_{\overline{\rho}}$ is a closed subfunctor represented by $R \in \mathcal{C}$ then the natural map $R^{\Box}_{\overline{\rho}} \to R$ is surjective.*

Proof. The map $R^{\Box}_{\overline{\rho}} \to R$ corresponds to the morphism of functors $D \to D^{\Box}_{\overline{\rho}}$. We have to show that if R' equals the image of this map then $R' = R$. This will follow if the representing object $\rho_D^{\mathrm{univ}} \in D(R)$ factors through $\mathrm{GL}_n(R')$. But this is clear since ρ_D^{univ} is obtained by applying $R^{\Box}_{\overline{\rho}} \to R$ to the representing object $\rho^{\mathrm{univ}} \in D^{\Box}_{\overline{\rho}}(R^{\Box}_{\overline{\rho}})$. □

In other words, $\operatorname{Spec} R \to \operatorname{Spec} R^{\Box}_{\overline{\rho}}$ is a closed immersion.

Proposition 35.4. *A subfunctor $D \to D^{\Box}_{\overline{\rho}}$ is closed if and only if $D = D^{\Box}_{\overline{\rho},\mathcal{Q}}$ for some deformation condition.*

Proof. If D is a closed subfunctor then say that $\rho : G \to \mathrm{GL}_n(A)$ has property $\mathcal{Q}_D$ if $\rho \in D(A)$. Then $D = D^{\Box}_{\overline{\rho},\mathcal{Q}_D}$.

Exercise 35.5. Show that if D is representable then $\mathcal{Q}_D$ is a deformation condition.

For the other direction suppose that $\mathcal{Q}$ is a deformation condition. Then representability of $D^{\Box}_{\overline{\rho},\mathcal{Q}}$ follows immediately from Schlessinger's criterion (or Grothendieck's representability theorem). This is because condition (3) ensures that the maps

$$D^{\Box}_{\overline{\rho},\mathcal{Q}}(A_1 \times_A A_2) \to D^{\Box}_{\overline{\rho},\mathcal{Q}}(A_1) \times_{D^{\Box}_{\overline{\rho},\mathcal{Q}}(A)} D^{\Box}_{\overline{\rho},\mathcal{Q}}(A_2)$$

are bijective or surjective precisely when they are when $D^{\Box}_{\overline{\rho},\mathcal{Q}}$ is replaced by $D^{\Box}_{\overline{\rho}}$. □

Finally, note that if $D_{\overline{\rho}}$ is representable then one can replace $D^{\Box}_{\overline{\rho}}$ by $D_{\overline{\rho}}$ in all the above results and definitions.

36. Examples: Fixed determinant

One example of a deformation condition is to fix the determinant of the deformations. One motivation for this construction comes from the use of deformation theory to study the representations of Galois groups associated to elliptic curves. One knows that (due to the Weil pairing) the determinant of any such representation is the cyclotomic character.

Construction 36.1. Fix a continuous character

$$\delta : G \to W(\mathbb{F})^\times$$

and define

$$D^\square_{\overline{\rho},\det=\delta}(A) \subset D^\square_{\overline{\rho}}(A)$$

as the subset consisting of ρ for which $\det\rho$ equals the character $G \overset{\delta}{\to} W(\mathbb{F})^\times \to A^\times$.

Lemma 36.2. *Assume that $\overline{\rho} \in D^\square_{\overline{\rho},\det=\delta}$. Then $D^\square_{\overline{\rho},\det=\delta}$ defines a deformation condition in $D^\square_{\overline{\rho}}$.*

Proof. Conditions (1) and (2) are immediately satisfied so we have to show that $\rho : G \to \mathrm{GL}_n(A \times B)$ has determinant δ if and only if the corresponding representations $\rho_A : G \to \mathrm{GL}_n(A)$ and $\rho_B : G \to \mathrm{GL}_n(B)$ have determinant δ. The only if direction is immediate since $\det\rho_A$ is the composite $G \xrightarrow{\det\rho} (A \times_C B)^\times \to A^\times$ (and likewise for B). For the if direction we observe that

$$\det\rho(g) = (\det\rho_A(g), \det\rho_B(g)) = (\delta(g), \delta(g))$$

□

Note that for any subfunctor $D \subset D^\square_{\overline{\rho}}$ we get an inclusion on tangent spaces:

$$D(\mathbb{F}[\epsilon]) \subset D^\square_{\overline{\rho}}(\mathbb{F}[\epsilon]) = Z^1(G, \mathrm{End}(\overline{\rho}))$$

In some cases it is also possible to give cohomological interpretations of these subspaces. For example:

Proposition 36.3. *Let $\mathrm{End}^0(\overline{\rho}) \subset \mathrm{End}(\overline{\rho})$ be the subspace consisting of trace zero matrices and write*

$$Z^1(G, \mathrm{End}^0(\overline{\rho})) = \{f \in Z^1(G, \mathrm{End}(\overline{\rho})) \mid f(g)\overline{\rho}(g)^{-1} \in \mathrm{End}^0(\overline{\rho})\}$$

. Then

$$D^\square_{\overline{\rho},\det=\delta}(\mathbb{F}[\epsilon]) = Z^1(G, \mathrm{End}^0(\overline{\rho}))$$

Proof. Recall that the identification

$$Z^1(G, \mathrm{End}(\overline{\rho})) \to D^\square_{\overline{\rho}}(\mathbb{F}[\epsilon])$$

sends f onto the deformation

$$\rho_f : g \mapsto \overline{\rho}(g) + \epsilon f(g)$$

We therefore just need to show that $\det \rho_f(g) = \delta(g)$ if and only if $f(g)\overline{\rho}(g)^{-1}$ has trace zero. But we can write

$$\det \rho_f(g) = \det \overline{\rho}(g) \det(1 + \epsilon\overline{\rho}(g)^{-1} f(g))$$

so we just need to show that $\det(1 + \epsilon\overline{\rho}(g)^{-1} f(g)) = 1$. But for any matrix one has

$$\det(1 + \epsilon A) = 1 + \mathrm{Tr}(A)$$

To see this just write $1+A = (a_{ij})$ so that the determinant is $\sum_\sigma \mathrm{sign}(\sigma) \prod_i a_{i,\sigma(i)})$. Note the only non-zero product occurs when $\sigma(i) = i$ for all i and so

$$\det(1 + \epsilon A) = \prod_{i=1}^{n} a_{i,i} = 1 + \mathrm{Tr}(A)$$

Thus $\det \rho_f = \delta$ if and only if $\mathrm{Tr}(\overline{\rho}(g)^{-1} f(g)) = \mathrm{Tr}(f(g)\overline{\rho}(g)^{-1}) = 0$. □

If we instead consider the case of unframed deformations we find

Corollary 36.4. *One has*

$$D_{\overline{\rho},\det=\delta}(\mathbb{F}[\epsilon]) = \mathrm{Im}\big(H^1(G, \mathrm{End}^0(\overline{\rho}) \to H^1(G, \mathrm{End}(\overline{\rho}))\big)$$

Proof. Recall that under the identifications $Z^1(G, \mathrm{End}(\overline{\rho})) = D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ and $H^1(G, \mathrm{End}(\overline{\rho})) = D_{\overline{\rho}}(\mathbb{F}[\epsilon])$ the map

$$D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon]) \to D_{\overline{\rho}}(\mathbb{F}[\epsilon])$$

sends $f \in Z^1(G, \mathrm{End}(\overline{\rho}))$ onto the class in $H^1(G, \mathrm{End}(\overline{\rho}))$ of the function $g \mapsto f(g)\overline{\rho}(g)^{-1}$. Thus, the image of $Z^1(G, \mathrm{End}^0(\overline{\rho}))$ under this map is precisely the image of $H^1(G, \mathrm{End}^0(\overline{\rho})) \to H^1(G, \mathrm{End}(\overline{\rho}))$. □

Exercise 36.5. Show that the map $\mathrm{Im}\big(H^1(G, \mathrm{End}^0(\overline{\rho}) \to H^1(G, \mathrm{End}(\overline{\rho}))\big)$ is injective when p does not divide n (here $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$) but need not be when p divides n.

We write $R^{\square}_{\overline{\rho},\det=\delta}$ for the ring representing $D^{\square}_{\overline{\rho},\det=\delta}$. Here is an explicit description of this ring:

Lemma 36.6.

$$R^{\square}_{\overline{\rho},\det=\delta} = R^{\square}_{\overline{\rho}}/I$$

where I is the ideal generated by $\delta(g) - \det \rho^{\mathrm{univ}}(g)$ for $\rho^{\mathrm{univ}} : G \to \mathrm{GL}_n(R^{\square}_{\overline{\rho}})$ the representing object.

Proof. We have to show that a map $R^{\square}_{\overline{\rho}} \to A$ factors through $R^{\square}_{\overline{\rho}}/I$ if and only if the composite

$$\rho_A : G \xrightarrow{\rho^{\mathrm{univ}}} \mathrm{GL}_n(R^{\square}_{\overline{\rho}}) \to \mathrm{GL}_n(A)$$

is contained in $D^{\square}_{\overline{\rho},\det=\delta}(A)$. But this is clear because $\det \rho_A(g) - \delta(g)$ equals the image of $\delta(g) - \det \rho^{\mathrm{univ}}(g)$ under $R^{\square}_{\overline{\rho}} \to A$. □

Finally, we prove a result which shows that one can easily recover $R^{\square}_{\overline{\rho}}$ from $R^{\square}_{\overline{\rho},\det=\delta}$ and vice-versa.

Proposition 36.7. *One has*

$$R^{\square}_{\overline{\rho}} \cong R_{\overline{\rho},\det=\delta}\widehat{\otimes}_{W(\mathbb{F})}R^{\square}_{\det\overline{\rho}}$$

Here the $\widehat{\otimes}$ *denotes the completed tensor product.*

Proof. The morphism of functors

$$D^{\square}_{\overline{\rho},\det=\delta} \times D^{\square}_{\det\overline{\rho}} \to D^{\square}_{\overline{\rho}}$$

given by $(\rho,\chi) \mapsto \rho\otimes\chi$ is an equivalence. Therefore one just need to show that $R_{\overline{\rho},\det=\delta}\widehat{\otimes}_{W(\mathbb{F})}R^{\square}_{\det\overline{\rho}}$ represents $D^{\square}_{\overline{\rho},\det=\delta} \times D^{\square}_{\det\overline{\rho}}$. This follows from the universal property for the tensor product: for $A \in \mathcal{C}^0$ a morphism $R_{\overline{\rho},\det=\delta}\widehat{\otimes}_{W(\mathbb{F})}R^{\square}_{\det\overline{\rho}} \to A$ is the same thing as a morphism $R_{\overline{\rho},\det=\delta}\otimes_{W(\mathbb{F})}R^{\square}_{\det\overline{\rho}}$, which is the same thing as a pair of morphisms of $W(\mathbb{F})$-algebras $R^{\square}_{\overline{\rho},\det=\delta} \to A$ and $R^{\square}_{\det\overline{\rho}} \to A$. □

37. Examples: Ordinary deformations

In this section we consider only the case of two dimensional representations. Then there is a notion of an ordinary Galois representation, which appears very frequently when considering Galois representations associated to certain modular forms and elliptic curves (though the precise definition often varies slightly). The definition we will use is:

Definition 37.1. Let $\rho : G \to \mathrm{GL}_2(R)$ be a continuous homomorphism with $R \in \mathcal{C}$ and let $I \subset G$ be closed subgroup. We say that ρ is I-ordinary if the submodule of I-fixed elements

$$\rho^I \subset \rho$$

(here we view ρ as R^2 equipped with an R-linear action of G) is R-free of rank one and is a direct summand. Equivalently, if ρ/ρ^I is R-free of rank one.

Motivation 37.2 (For those who know something about modular forms)**.** Here is an example where ordinary Galois representations appear in "nature". Let f be a Hecke eigenform whose U_p-eigenvalue has p-adic valuation 0 (i.e. is a p-adic unit). Then the corresponding p-adic Galois representation

$$\rho_f : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathcal{O})$$

(here S is some finite set of places containing p and $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}_p$) is ordinary at $I_p \subset G_{\mathbb{Q}_p} \subset G_{\mathbb{Q},S}$.

Proposition 37.3. *If* $\overline{\rho}$ *is* I*-ordinary then the condition of being* I*-ordinary is a deformation condition on* $D^{\square}_{\overline{\rho}}$.

Proof. It is easy to see that if $\rho : G \to \mathrm{GL}_2(A)$ is I-ordinary then so is its image under a morphsim $A \to B$ in $\mathcal{C}^0$ (since ρ being I-ordinary just means there exists $Y \in \mathrm{GL}_2(A)$ so that $\rho(g) = Y\begin{pmatrix}1 & * \\ 0 & *\end{pmatrix}Y$ for every $g \in I$). Therefore, the main thing is to check that if

$$\rho : G \to \mathrm{GL}_2(A \times_C B)$$

is such that ρ_A and ρ_B are I-ordinary then ρ is I-ordinary. Since ρ_A and ρ_B are I-ordinary we can find I-invariant elements $e_A \in A^2$ and $e_B \in B^2$ which generate a direct summand. The images of e_A and e_B in C^2 must then generate the same C-submodule and so, after possibly multiplying e_B with a unit, we can assume that e_A and e_B are equal in C^2. Therefore

$$(e_A, e_B) \in (A \times_C B)^2$$

is an I-fixed element. It also generates a direct summand of $(A \times_C B)^2$ because we can choose splittings of $Ae_A \to A^2$ and $Be_B \to B^2$ which are equal after base-change to C. Thus, we obtain a splitting of $A \times_C B(e_A, e_B) \to (A \times_C B)^2$. □

Remark 37.4. As with $D_{\overline{\rho},\det=\delta}$ there is an explicit description of the I-ordinary deformation ring $R^{\square}_{\overline{\rho},I}$ as a quotient of $R^{\square}_{\overline{\rho}}$. For this suppose that

$$\overline{\rho}(g) = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

for $g \in I$. Then $R^{\square}_{\overline{\rho},I} = R^{\square}_{\overline{\rho}}/I$ for I the ideal generated by

$$a_{21}(g), a_{11}(g) - 1, \qquad g \in I$$

for $\rho^{\text{univ}}(g) = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$.

Write $D^{\square}_{\overline{\rho},I}$ for the subfunctor of I-ordinary deformations. One can also produce a cohomological description of the tangent space

$$D^{\square}_{\overline{\rho},I}(\mathbb{F}[\epsilon])$$

For this set $\text{End}_I(\overline{\rho}) \subset \text{End}(\overline{\rho})$ equal to the set of endomorphism which factor through ρ/ρ^I (in other words, are zero on ρ^I). Define

$$Z^1(G, \text{End}_I(\overline{\rho})) = \{f \in Z^1(G, \text{End}(\overline{\rho})) \mid f(g) \in \text{End}_I(\overline{\rho}) \text{ for } g \in I\}$$

Lemma 37.5. *Under the identification $Z^1(G, \text{End}(\overline{\rho})) = D^{\square}_{\overline{\rho}}(\mathbb{F}[\epsilon])$ one has*

$$Z^1(G, \text{End}_I(\overline{\rho})) = D^{\square}_{\overline{\rho},I}(\mathbb{F}[\epsilon])$$

Proof. This is obvious. □

38. Examples: Categorical deformation conditions

Several important deformation conditions (particularly those coming from p-adic Hodge theory) can be described in the following way:

Definition 38.1. Let $\mathcal{P}$ be a full-subcategory of the category of finite length $W(\mathbb{F})$-modules equipped with a continuous action of G. For $A \in \mathcal{C}^0$ set

$$D^{\square}_{\overline{\rho},\mathcal{P}}(A) = \{\rho \in D^{\square}_{\overline{\rho}}(A) \mid \rho \in \mathcal{P}\}$$

(here we identify ρ with the module A^n with G-action induced by ρ).

Proposition 38.2. *Suppose that $\mathcal{P}$ is closed under passage to subobjects, quotients and finite direct sums. If $\overline{\rho} \in \mathcal{P}$ then $D^{\square}_{\overline{\rho},\mathcal{P}}$ is a deformation condition.*

Proof. Let $A \to B$ be a morphism in $\mathcal{C}^0$ and suppose $\rho \in D^{\square}_{\overline{\rho},\mathcal{P}}(A)$. The first thing to show is that the image $\rho_B \in D^{\square}_{\overline{\rho}}(B)$ is an object of $\mathcal{P}$. To do this we factor $A \to B$ through C so that

- C is free as an A-module.
- $C \to B$ is surjective.

One way to produce such a C is to consider a surjection $A[[X_1, \dots, X_n]] \to B$ and take C equal to a quotient of $A[[X_1, \dots, X_n]]$ by a sufficiently large power of its maximal ideal. Let $\rho_C \in D^{\square}_{\overline{\rho}}(C)$ be the image of ρ. Since C is free as an A-module we can identify

$$\rho_C = \rho^{\oplus \operatorname{rank}_A C}$$

as A-modules. Since $\mathcal{P}$ is closed under finite direct sums it follows that $\rho_C \in \mathcal{P}$. Since $C \to B$ is surjective it follows also that $\rho_C \to \rho_B$ is a surjection of G-modules. Since $\mathcal{P}$ is closed under quotients it follows that $\rho_B \in \mathcal{P}$ also.

We also need to prove that if $\rho \in D^{\square}_{\overline{\rho}}(A \times_C B)$ has images ρ_A and ρ_B in $D^{\square}_{\overline{\rho},\mathcal{P}}(A)$ and $D^{\square}_{\overline{\rho},\mathcal{P}}(B)$ respectively then $\rho \in \mathcal{P}$. To see this note that $A \times_C B$ is a subring of $A \oplus B$ and therefore

$$\rho \subset \rho_A \oplus \rho_B$$

Since $\mathcal{P}$ is closed under finite direct sums and subobjects we conclude $\rho \in \mathcal{P}$ also. □

Lecture 18

39. Categorical deformation conditions (continued)

The most important example of a categorical deformation condition appears when $G = G_K$ for K a finite extension of $\mathbb{Q}_p$ and $\mathbb{F}$ has characteristic p, i.e. in the p-adic setting. In this case one takes $\mathcal{P}$ to be the full subcategory of *flat* representations.

To explain what this means one considers a collection of objects called finite flat group schemes. By definition these are affine group schemes over $\mathcal{O}_K$ whose coordinate rings are finite and flat as an $\mathcal{O}_K$-algebra. One considers the abelian category $\underline{\mathrm{FFgs}}_{\mathcal{O}_K}$ of such group schemes which are also commutative and of order a power of p. One can make the same construction with $\mathcal{O}_K$ replaced by K, and in this case one has an (exact) equivalence of categories

$$\underline{\mathrm{Ffgs}}_K \cong \{\text{finite length } \mathbb{Z}_p\text{-modules equipped with a continuous } G_K\text{-action}\}$$

given by $\mathcal{G}_K \mapsto \mathcal{G}_K(\overline{K})$. One can then consider the composite

$$\underline{\mathrm{Ffgs}}_{\mathcal{O}_K} \to \underline{\mathrm{Ffgs}}_K \to \text{ finite length } \mathbb{Z}_p\text{-modules equipped with a continuous } G_K\text{-action}$$

with the first arrow given by base-change $\mathcal{G} \mapsto \mathcal{G} \times_{\mathcal{O}_K} K$. It turns out that asking for a finite flat group scheme over K to extend to $\mathcal{O}_K$ (i.e. arise by base-change from one over $\mathcal{O}_K$) is a strong condition and one says that a representation of G_K on a finite length $\mathbb{Z}_p$-module is flat if it is contained in the essential image of this composite of functors.

Example 39.1. The reason why being flat is significant is because if E is an elliptic curve over $\mathcal{O}_K$ then the G_K-representation $E[p^n](\overline{K})$ given by its p^n-torsion points is flat.

Proposition 39.2. *The collection of flat deformations is a deformation condition. Thus, there exists a quotient $R^{\square}_{\overline{\rho},\mathrm{flat}}$ of $R^{\square}_{\overline{\rho}}$ such that a morphism $R^{\square}_{\overline{\rho}} \to A$ with $A \in \mathcal{C}^0$ factors through $R^{\square}_{\overline{\rho},\mathrm{flat}}$ if and only if $\rho^{\mathrm{univ}} \otimes_{R^{\square}_{\overline{\rho}}} A$ is flat.*

Sketch of proof. Recall we just have to show that the category of flat G_K-representation is stable under subobjects, quotients, and finite direct sums. Let us just sketch how one shows it is stable under subobjects. Stability under quotients is similar and stability under direct sums is much easier. If V is flat then $V = \mathcal{G}(\overline{K})$ for a finite flat group scheme $\mathcal{G}$ over $\mathcal{O}_K$. If $V' \subset V$ is a subobject then $V' = \mathcal{G}'_K(\overline{K})$ for a subobject $\mathcal{G}'_K \subset \mathcal{G} \times_{\mathcal{O}_K} K$. Set $\mathcal{G}'$ equal to the closure of $\mathcal{G}'_K$ inside $\mathcal{G}$. One shows that this closure is again a group scheme (if it is then it is clearly an object of $\underline{\mathrm{Ffgs}}_{\mathcal{O}_K}$) and so V' is flat. □

40. Example: Global deformation conditions at each prime

Here let we consider a global situation. For simplicity we work over the rational numbers and let $G = G_{\mathbb{Q},S}$ for S a finite set of rational primes. Particularly for applications to modularity lifting theorems one often wants to consider deformations of a $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathbb{F})$ where one imposes conditions on the restriction of deformations of $\overline{\rho}$ to the local Galois groups $G_{\mathbb{Q}_l} \subset G_{\mathbb{Q},S}$ for all primes $l \in S$.

Motivation 40.1. Suppose one wants to study the Galois representation coming from the Tate-module $T(E) := \varprojlim_n E[p^n](\overline{\mathbb{Q}})$ of an elliptic curve E using deformation theory. Usually one wants to make the corresponding deformation space as small as possible by imposing as many conditions as possible which are satisfied by $T(E)$. Here one takes S the set containing the primes of bad reduction of E and p; this ensures that $T(E)$ induces a representation of $G_{\mathbb{Q},S}$. Then one knows

- for $l \neq p$ conditions on the action of $G_{\mathbb{Q}_l} \subset G_{\mathbb{Q},S}$ on $T(E)$ in terms of the conductor of E;
- that $T(E)$ is flat when viewed as a $G_{\mathbb{Q}_p}$-representation.

Both of these points are deformation conditions (we've seen this for flatness condition at p) so we would like to study deformations of the reduction modulo p of $T(E)$ which satisfy these local properties.

Definition 40.2. Let $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathbb{F})$ be continuous. Then a global deformation problem $\mathcal{Q}$ is a collection of deformation problems $\mathcal{Q}_l$ for each $l \in S$. We say a deformation $\rho \in D^{\square}_{\overline{\rho}}(A)$ has $\mathbb{Q}$ if the composite $G_{\mathbb{Q}_l} \to G_{\mathbb{Q},S} \xrightarrow{\rho} \mathrm{GL}_n(A)$ has $\mathcal{Q}_l$ for every $l \in S$.

Lemma 40.3. *Any global deformation $\mathcal{Q}$ problem is a deformation problem in the sense of Definition 35.1.*

Proof. This is easy. For example if $\rho \in D^{\square}_{\overline{\rho}}(A \times_B C)$ with images $\rho_A \in D^{\square}_{\overline{\rho}}(A)$ and $\rho_B \in D^{\square}_{\overline{\rho}}(B)$ then ρ has property $\mathcal{Q}$ if and only if the restriction of ρ to $G_{\mathbb{Q}_l}$ as property $\mathcal{Q}_l$ for every $l \in S$. Since each $\mathcal{Q}_l$ is a deformation condition this is equivalent to the restrictions of ρ_A and ρ_B having properties $\mathcal{Q}_l$ for every $l \in S$, which is in turn equivalent to ρ_A and ρ_B having property $\mathcal{Q}$. □

Now suppose that $\operatorname{End}(\overline{\rho}) = \mathbb{F}$ so that we can drop the framing in the above discussion.

Proposition 40.4. *Let $\mathcal{Q}$ be a global deformation problem and write*

$$H^1_{\mathcal{Q}_l}(G_{\mathbb{Q}_l}, \operatorname{End}(\overline{\rho})) \subset H^1(G_{\mathbb{Q}_l}, \operatorname{End}(\overline{\rho}))$$

for the subspace determined by the tangent space $D_{\overline{\rho},\mathbb{Q}_l}(\mathbb{F}[\epsilon])$. Then $D_{\overline{\rho},\mathbb{Q}}(\mathbb{F}[\epsilon])$ equals the "Selmer group" which is the preimage of

$$\bigoplus_{l \in S} H^1_{\mathbb{Q}_l}(G_{\mathbb{Q}_l}, \operatorname{End}(\overline{\rho}))$$

under the map $H^1(G_{\mathbb{Q},S}, \operatorname{End}(\overline{\rho})) \to \bigoplus_{l \in S} H^1(G_{\mathbb{Q}_l}, \operatorname{End}(\overline{\rho}))$ obtained as the direct sum of restriction maps.

Proof. This is clear. □

41. Lifting criteria and flatness

Suppose one has a continuous representation $\overline{\rho} : G \to \operatorname{GL}_n(\mathbb{F})$. Let $p = \operatorname{char} \mathbb{F}$. Then a natural question is whether there exists a lift of $\overline{\rho}$ to a representation $\rho : G \to \operatorname{GL}_n(\mathcal{O})$ where $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}$ with residue field $\mathbb{F}$. Unsurprisingly, the answer to this question can be seen from the deformation ring. One direction is easy:

Example 41.1. Suppose that $R^{\square}_{\overline{\rho}}$ represents $D^{\square}_{\overline{\rho}}$ and that $R^{\square}_{\overline{\rho}}$ is p-power torsion. In other words assume that $p^n R^{\square}_{\overline{\rho}} = 0$ for some $n \geq 1$. Then there can be no lift of $\overline{\rho}$ to $\rho : G \to \operatorname{GL}_n(\mathcal{O})$ with $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}$ because any such lift would correspond to a homomorphism $R^{\square}_{\overline{\rho}} \to \mathcal{O}$. If $R^{\square}_{\overline{\rho}}$ is killed by p^n then any such homomorphism must be zero.

In fact, this is an if and only if.

Proposition 41.2. *Let R be a complete local Noetherian ring with residue field $\mathbb{F}$. Then there exists a local homomorphism $R \to \mathcal{O}$ inducing a non-zero map on residue fields, with $\mathcal{O}$ the ring of integers in some finite extension of $\mathbb{Q}_p$, if and only if $R[\frac{1}{p}] \neq 0$.*

First we prove two lemmas:

Lemma 41.3. *Let R be a Noetherian domain and suppose $R[\frac{1}{f}]$ is a field. Then R has Krull dimension ≤ 1.*

Proof. Since $R[\frac{1}{f}]$ is a field every non-zero prime ideal contains f. Let $\mathfrak{p}_i$ be the primes of A minimal non-zero prime ideals. It suffices to show these are all maximal. If $\mathfrak{p}_j$ is not maximal choose a maximal ideal containing it $\mathfrak{m}$. Then $\mathfrak{p}_i \subset \mathfrak{m}$ for any i and so $\mathfrak{m}$ is not contained in $\bigcup_i \mathfrak{p}_i$ by Prime avoidance. Therefore, there is $g \in \mathfrak{m}$ not contained in any $\mathfrak{p}_i$.

Choose $\mathfrak{q}$ a minimal prime containing g. Then Theorem 32.5 implies there is no non-zero prime $\mathfrak{p} \subset \mathfrak{q}$. However, $\mathfrak{q} \neq 0$ so $\mathfrak{p}_i \subset \mathfrak{q}$ for some i. This is not an equality because $g \in \mathfrak{q}$ but not in $\mathfrak{p}_i$. This gives a contradiction. □

Corollary 41.4. *Suppose that R is a local integral domain with $pR \neq 0$ and residue field a finite extension of $\mathbb{F}_p$. If $R[\frac{1}{p}]$ is a field then $R[\frac{1}{p}]$ is a finite extension of $\mathbb{Q}_p$ and R is contained in the ring of integers of this finite extension.*

Proof. The previous lemma shows that R has Krull dimension ≤ 1. Therefore R/p has Krull dimension 0 and so is an Artin local ring with finite residue field. In particular it is finite generated over $\mathbb{Z}_p$ which shows that R is also finitely generated over $\mathbb{Z}_p$. It follows that $R[\frac{1}{p}]$ is finitely generated over $\mathbb{Q}_p$ and that R is contained in the ring of integers of this finite extension. □

Proof of Proposition. Note that $R[\frac{1}{p}] = 0$ implies $p^n R = 0$ for some $n \geq 1$ so we've just seen one direction. For the opposite direction, we can replace R by R/I where I denotes the ideal of elements killed by some power of p. This means that the map $R \to R[\frac{1}{p}]$ is an inclusion.

Choose a maximal ideal Q in $R[\frac{1}{p}]$ and set $P = Q \cap R$ which is a prime ideal in R. Since $R[\frac{1}{p}]/Q = (R/P)[\frac{1}{p}]$, the previous corollary applied to R/P shows that R/P is contained in the ring of integers of the finite extension $R[\frac{1}{p}]/Q$ of $\mathbb{Q}_p$. If $\mathcal{O}$ denotes this ring of integers then we obtain a homomorphism

$$R \to R/P \hookrightarrow \mathcal{O}$$

and we are done. □

So roughly, a deformation ring being flat over $\mathbb{Z}_p$ (i.e. p-torsionfree) is roughly the same as saying you can always construct lifts to characteristic zero. However, you have to be a little careful here because certainly flatness is not as strong a condition as being formally smooth. Here is technical result which makes this slogan slightly more precise:

Proposition 41.5. *Let R be a complete Noetherian local $\mathbb{Z}_p$-algebra with finite residue field. Assume that R is p-torsionfree and $R[\frac{1}{p}]$ is reduced. For any ideal $I \subset R$ containing p there exists a finite flat $\mathbb{Z}_p$-algebra C such that $R \to R/I$ factors through $A \to C$.*

Proof. We can assume that $I = \mathfrak{m}_R^j$ for some $j \geq 1$. The first thing we use is that $R[\frac{1}{p}]$ being reduced implies $\bigcap \mathfrak{p} = 0$ with the intersection running over all maximal ideals in $R[\frac{1}{p}]$. This is the case in any reduced ring which is Jacobson (which means that every prime ideal is the intersection of the maximal ideals containing it). It is a theorem (see Tag 02IM of the stacks project) that if A is a Noetherian local ring then $\operatorname{Spec} A \smallsetminus \{\mathfrak{m}_A\}$ is a Jacobson scheme (i.e. every affine open in this scheme is spec of a Jacobson ring). In particular $R[\frac{1}{p}]$ is Jacobson which proves our claim. It follows also that

$$\bigcap(\mathfrak{p} \cap R) = 0$$

with the intersection running over maximal ideals in $R[\frac{1}{p}]$.

We can refine this assertion slightly: let $\mathfrak{p}_1, \mathfrak{p}_2, \dots$ be a sequence of distinct maximal ideals in $R[\frac{1}{p}]$. Then we claim that

$$\bigcap_i(\mathfrak{p}_i \cap R) = 0$$

also. To see this one writes $\mathfrak{p} \cap R = \bigcap_j \left(\mathfrak{p} \cap R + \mathfrak{m}_R^j\right)$ so that

$$\bigcap(\mathfrak{p} \cap R) = \bigcap_{\mathfrak{p},n} \left(\mathfrak{p} \cap R + \mathfrak{m}_R^j\right)$$

However, for fixed n the collection of ideals of the form $\left(\mathfrak{p} \cap R + \mathfrak{m}_R^j\right)$ contains finitely many distinct elements. This shows that the previous intersection runs over countably many distinct ideals. Hence we can choose an indexing as claimed.

If we set $\mathfrak{q}_j = \bigcap_{i=1}^j (\mathfrak{p}_i \cap R)$ then these form a sequence of decreasing ideals in A whose intersection is zero. A general result about complete Noetherian rings implies that $\mathfrak{q}_n \subset \mathfrak{m}_j$ for $n >> 0$. Hence $R \to R/\mathfrak{m}_R^j$ factors through $C = R/\mathfrak{q}_n$ for $n >> 0$. Therefore, we just need to show that $R/\mathfrak{q}_n$ is finite flat over $\mathbb{Z}_p$. This follows since there is an embedding

$$R/\mathfrak{q}_n \hookrightarrow \prod_{i=1}^n R/(\mathfrak{p}_i \cap R)$$

with target finite and flat over $\mathbb{Z}_p$ (by the corollary above).

□

Part 1. Lecture 20

42. Setup for l-adic deformations

The main goal for the rest of the course is to carefully study the l-adic deformation theory of two dimensional representations of G_K for $K/\mathbb{Q}_p$ a finite extension with $l \neq p$. For the we remind ourselves of the basic structure of this group and fix some notation:

- Let $I_K \subset G_K$ denote the inertia subgroup so that $G_K/I_K \cong \widehat{Z}$.
- Let $P_K \subset G_K$ denote the wild inertia subgroup. This is a pro-p-group normal in G_K with $I_K/P_K \cong \prod_{l' \neq p} \mathbb{Z}_{l'}$.
- Define $\widetilde{P}_K \subset I_K$ so that $I_K/\widetilde{P}_K \cong \mathbb{Z}_l$ is the maximal pro-l quotient of I_K. Thus $\widetilde{P}_K$ has order prime to l. Note also that $\widetilde{P}_K$ is normal in G_K.

We also fix a finite field $\mathbb{F}$ of characteristic $l \neq p$ and $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$. Soon we will take $n = 2$.

43. Removing prime-to-l ramification

Our goal here is to reduce the calculation of $R^{\square}_{\overline{\rho}}$ to the case where $\overline{\rho}|_{\widetilde{P}_K}$ is the trivial representation.

To do this we first consider an $\mathbb{F}$-representation of M of $\widetilde{P}_K$ and evaluation gives a map

$$\bigoplus_{\theta} \theta \otimes M_\theta \to M, \qquad M_\theta := \operatorname{Hom}_{\widetilde{P}_K}(\theta, M)$$

with the direct sum running over isomorphism classes of irreducible $\mathbb{F}$-representations of $\widetilde{P}_K$. Since $\widetilde{P}_K$ has order prime to the characteristic of $\mathbb{F}$ all such representations are semi-simple and so this map is an isomorphism. In fact, a similar decomposition applies when M is a representation of $\widetilde{P}_K$ on a finite $W(\mathbb{F})$-module.

Lemma 43.1. *Suppose that θ is an irreducible $\mathbb{F}$-representation of $\widetilde{P}_K$. Then there exists a continuous representation $\widetilde{\theta} : \widetilde{P}_K \to \mathrm{GL}_n(W(\mathbb{F}))$ such that*

$$\widetilde{\theta}|_{\widetilde{P}_K} \cong \theta \textit{ modulo } l$$

Proof. This will follow if we can show that the deformation ring of θ is a power series ring over $W(\mathbb{F})$. We know this follows if we can show $H^2(\widetilde{P}_K, \operatorname{End}\theta) = 0$. This is the case because $\widetilde{P}_K$ has order prime to l. In fact in this situation all high cohomologies vanish. Here is a sketch of why this occurs: choose a presentation $\widetilde{P}_K \cong \varprojlim N_i$ with N_i finite quotients of $\widetilde{P}_K$ acting trivially on $\operatorname{End}\theta$. Then

$$H^i(\widetilde{P}_K, \operatorname{End}\overline{\rho}) \cong \varinjlim H^i(N_j, \operatorname{End}\overline{\rho})$$

so it suffices to show $H^i(N, M) = 0$ for $i > 0$ when N is a finite group of order n and multiplication by n is injective on M. For this consider the restriction and corestriction maps

$$\operatorname{res} : H^i(N, M) \to H^i(\{1\}, M) = 0, \qquad \operatorname{cores} : H^i(\{1\}, M) = 0 \to H^i(N, M)$$

Since $\operatorname{res} \circ \operatorname{cores}$ equals multiplication by n it follows that res is injective and so $H^i(N, M) = 0$. □

Remark 43.2. The lifting here is unique up to conjugation because $H^1(\widetilde{P}_K, \operatorname{End}\theta) = 0$ and so the deformation ring is $W(\mathbb{F})[[x_1, \ldots, x_{n^2}]]$ with the variable coming from conjugation.

For each irreducible $\widetilde{P}_K$-representation θ choose a $\widetilde{\theta}$ as in the lemma. If M is any finite $W(\mathbb{F})$-module equipped with an action of $\widetilde{P}_K$ we have a map

$$\bigoplus_{\theta} \widetilde{\theta} \otimes M_\theta \to M, \qquad M_\theta := \operatorname{Hom}_{\widetilde{P}_K}(\widetilde{\theta}, M)$$

which generalises the previous one. Note that these maps are compatible with exact sequences in M. As $M \mapsto \operatorname{Hom}_{\widetilde{P}_K}(\widetilde{\theta}, M)$ is exact, since $\widetilde{\theta}$ is $W(\mathbb{F})$-free, the fact this map is an isomorphism for l-torsion M implies that it is also for general $W(\mathbb{F})$-finite M by an inductive argument.

Proposition 43.3. *Now suppose M is a representation of G_K on a finite $W(\mathbb{F})$-module. For each θ as above set*

$$G_\theta = \{g \in G_K \mid g\theta g^{-1} \cong \theta\}$$

and choose a lift $\widetilde{\theta}$. Then $\widetilde{\theta}$ extends to a representation of G_θ and there are functorial (in M) isomorphisms

$$M \cong \bigoplus_{[\theta]} \operatorname{Ind}_{G_\theta}^{G_K}(\widetilde{\theta} \otimes M_\theta)$$

where the sum runs over G_K-conjugacy classes of θ. Here the G_θ-action on M_θ is defined by $(gf)(v) = gf(g^{-1}v)$.

Proof. We leave the proof that $\widetilde{\theta}$ extends to a representation of G_θ. See Lemma 2.4.11 of Clozel–Harris–Taylor "Automorphy of some l-adic lifts of automorphic mod l representations".

Granting this extension for each θ, we see that the evaluation map $\widetilde{\theta} \otimes M_\theta \to M$ is G_θ-equivariant since

$$g \cdot (v, f) = (gv, g \cdot f) \mapsto gf(g^{-1}gv) = gf(v)$$

for $g \in G_\theta$. Frobenius reciprocity therefore gives a G_K-equivariant map

$$\bigoplus_{[\theta]} \operatorname{Ind}_{G_\theta}^{G_K}(\widetilde{\theta} \otimes M_\theta) \to M \tag{43.4}$$

We will be done if we can show that after restricting to $\widetilde{P}_K$ this is the map defined above. For this note that Mackey's theorem implies

$$\operatorname{Ind}_{G_\theta}^{G_K}(\widetilde{\theta} \otimes M_\theta)|_{\widetilde{P_K}} \cong \bigoplus_{g \in G_K/G_\theta} (\widetilde{\theta} \otimes M_\theta)^g$$

where the superscript g indicates the g-conjugate representation. Since $(\widetilde{\theta} \otimes M_\theta)^g = \widetilde{\theta}^g \otimes M_{\theta^g}$ the source of can be written as

$$\bigoplus_{\theta} \widetilde{\theta} \otimes M_\theta$$

as a $\widetilde{P}_K$-representation, with the sum running isomorphism classes of θ's. One then just has to check that under this identification (43) coincides with our previous map. □

We can use this to say something about the (unframed) deformation functor $D_{\overline{\rho}}$:

Corollary 43.5. *Suppose $A \in \mathcal{C}$. Then the map*

$$\rho \mapsto (\rho_\theta)_{[\theta]}$$

defines a bijection between $D_{\overline{\rho}}(A)$ and tuples of deformations of the G_θ-representations $\overline{\rho}_\theta$ as θ runs over G_K-conjugacy classes of irreducible $\widetilde{P_K}$-representations.

Proof. If A is Artinian this follows from the previous proposition and the case of general A follows my a limit argument. □

In other words, we have an isomorphism of functors

$$D_{\overline{\rho}} \cong \prod_{[\theta]} D_{\overline{\rho}_\theta}$$

If each of these functors is representable then it follows that

$$R_{\overline{\rho}} \cong \widehat{\bigotimes}_{[\theta]} R_{\overline{\rho}_\theta}$$

Furthermore, if $\rho_\theta^{\mathrm{univ}}$ is the universal object representing $D_{\overline{\rho}_\theta}$ then

$$\rho^{\mathrm{univ}} = \bigoplus_{[\theta]} \mathrm{Ind}_{G_\theta}^{G_K}(\widetilde{\theta} \otimes \rho_\theta^{\mathrm{univ}})$$

represents $D_{\overline{\rho}}$. Note this reduced the problem of computing deformations to the case where the action of $\widetilde{P}_K$ acts as the identity. We need an extra argument to upgrade this to an isomorphism of framed deformation rings (this comes down to keeping track of choices of bases).

Proposition 43.6. *One has*

$$R_{\overline{\rho}}^{\square} \cong \left(\widehat{\bigotimes}_{[\theta]} R_{\overline{\rho}_\theta}^{\square}\right)[[X_1, \ldots, X_{n^2 - \sum n_\theta^2}]]$$

where $n_\theta = \dim \theta$.

Proof. Let ρ^{univ} be the representing object of $D_{\overline{\rho}}^{\square}$. The above gives that

$$\rho^{\mathrm{univ}} \cong \bigoplus_{[\theta]} \mathrm{Ind}_{G_\theta}^{G_K}(\widetilde{\theta} \otimes \rho_\theta^{\mathrm{univ}})$$

and so, after restricting to $\widetilde{P}_K$, we have $\rho^{\mathrm{univ}} \cong \bigoplus_\theta \widetilde{\theta} \otimes \rho_\theta^{\mathrm{univ}}$ (θ here running over isomorphism classes rather than G_K-conjugacy classes). Therefore we can write ρ^{univ} as

$$\rho^{\mathrm{univ}} \sim Y \begin{pmatrix} ()_{\theta_1} & & & \\ & ()_{\theta_2} & & \\ & & \ddots & \\ & & & ()_{\theta_J} \end{pmatrix} Y^{-1}$$

for some $Y \in 1 + \mathrm{Mat}(\mathfrak{m}_{\overline{\rho}})$. The θ'th block gives a choice of basis on $\widetilde{\theta} \otimes \rho_\theta^{\mathrm{univ}}$. Replacing Y if necessary we can assume this choice of basis comes from the tensor product of a choice of basis on $\widetilde{\theta}$ and one on $\rho_\theta^{\mathrm{univ}}$.

Note that $\rho_\theta^{\mathrm{univ}}$ is an unframed deformation of $\overline{\rho}_\theta$ but the choice we just made allows us to upgrade it into a framed deformation. Thus, we obtain a morphism

$$\widehat{\bigotimes}_{[\theta]} R_{\overline{\rho}_\theta}^{\square} \to R_{\overline{\rho}}^{\square}$$

and we want to show this is formally smooth. In other words, if we have a commutative diagram

$$\begin{tikzcd} \widehat{\otimes}_{[\theta]} R_{\overline{\rho}_\theta}^{\square} \arrow[r] \arrow[d] & R_{\overline{\rho}}^{\square} \arrow[d] \\ A \arrow[r] & B \end{tikzcd}$$

with $A \to B$ in $\mathcal{C}^0$ then we can construct an arrow $R^{\square}_{\overline{\rho}} \to A$ making the diagram commute.

The right horizontal arrow corresponds to a framed deformation ρ_B of $\overline{\rho}$ to B. The left horizontal arrow corresponds to a tuple of framed deformations (ρ_θ) to A from this we produce an unframed deformation

$$\rho_A := \bigoplus_{[\theta]} \operatorname{Ind}_{G_\theta}^{G_K}(\widetilde{\theta} \otimes \rho_\theta)$$

of $\overline{\rho}$ lifts ρ_B. Lifting the choice of basis on ρ_B we can make this into framed deformation which produces a map $R^{\square}_{\overline{\rho}} \to A$ making the bottom triangle in the square commute. Note that the top triangle may not commute because our lift of the basis on ρ_B to ρ_A need not be compatible with the framings on ρ_θ determined by the map $\widehat{\bigotimes}_{[\theta]} R^{\square}_{\overline{\rho}_\theta} \to A$.

Exercise 43.7. Using that the whole square commutes show that one can make such a choice of lift of bases so that the top triangle commutes.

The formal smoothness implies that $R^{\square}_{\overline{\rho}} \cong \left(\widehat{\bigotimes}_{[\theta]} R^{\square}_{\overline{\rho}_\theta}\right)[[X_1, \dots, X_N]]$ for some N. To show that $N = n^2 - \sum n_\theta^2$ we look at the dimensions of the mod p tangent spaces. The mod p tangent space of the source has dimension

$$\dim_{\mathbb{F}} D_{\overline{\rho}}(\mathbb{F}[\epsilon]) + n^2 - \dim H^0(G_K, \operatorname{End}(\overline{\rho}))$$

while that of the target is

$$N + \sum_{[\theta]} \left(\dim_{\mathbb{F}} D_{\overline{\rho}_\theta}(\mathbb{F}[\epsilon]) + n_\theta^2 - \dim H^0(G_K, \operatorname{End}(\overline{\rho}_\theta))\right)$$

So we just need to show that $\sum_{[\theta]} \dim H^0(G_K, \operatorname{End}(\overline{\rho}_\theta)) = \dim H^0(G_K, \operatorname{End}(\overline{\rho}))$. But this is clear from the definition of $\overline{\rho}_\theta$. □

44. First application

Now assume $n = 2$ and that $\overline{\rho}|_{\widetilde{P}_K}$ is irreducible. Call this irreducible representation θ. Then ρ_θ is one dimensional and the previous proposition gives that

$$R^{\square}_{\overline{\rho}} \cong R^{\square}_{\overline{\rho}_\theta}[[X_1, X_2, X_3]]$$

Since every G_K conjugate of θ must be an irreducible factor of $\overline{\rho}_{\widetilde{P}_K}$ we know that any such conjugate is isomorphic to θ. Hence $G_\theta = G_K$. Thus, we've just reduced everything to the calculation of a one-dimensional deformation ring. We know such a ring is isomorphic to

$$W(\mathbb{F})[[X, Y]]/((1+X)^{l^a} - 1)$$

where a denotes the l-adic valuation of $\operatorname{Card}(k^\times)$. Therefore:

Proposition 44.1. *If $\overline{\rho}|_{\widetilde{P}_K}$ is irreducible then*

$$R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[X_1, X_2, X_3, X_4, Y]]/((1+Y)^{l^a} - 1)$$

The universal deformation is equal to $\widetilde{\theta} \otimes \chi^{\text{univ}}$ where χ^{univ} is the universal deformation of ρ_θ.

Lecture 21

In this lecture the set-up is the same as that in the previous one. Thus $K/\mathbb{Q}_p$ is a finite extension with residue field k and $\mathbb{F}$ is a finite field of characteristic $l \neq p$ with $l > 2$. We have fixed a continuous representation $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ and for today we consider only the case $n - 2$.

Recall that $\widetilde{P}_K$ denotes the prime-to-l part of I_K

45. Non-trivial prime to l-inertia

We previously treated the case where $\overline{\rho}|_{\widetilde{P}_K}$ was irreducible. The other possibility is that $\overline{\rho}|_{\widetilde{P}_K} \cong \theta_1 \oplus \theta_2$. Recall that Proposition 43.3 ensures each θ_i lifts to $W(\mathbb{F})$-valued characters $\widetilde{\theta}_i$ and that each $\widetilde{\theta}_i$ extends to a character of G_{θ_i} which is defined as the stabiliser of θ_i under the action of G_K on the irreducible constituents of $\overline{\rho}|_{\widetilde{P}_K}$.

Let us first consider the case $\theta_1 \neq \theta_2$. Then there are two cases:

- θ_1 and θ_2 are not G_K-conjugate. Then $G_{\theta_i} = G_K$ and so each $\widetilde{\theta}_i$ extends to characters of G_K. Then Proposition 43.6 implies that
$$R^{\square}_{\overline{\rho}} \cong \left(R^{\square}_{\theta_1} \widehat{\otimes} R^{\square}_{\theta_2}\right)[[Z_1, Z_2]]$$
- θ_1 and θ_2 are conjugate and $G_\theta = G_L$ for L/K a degree two extension. Since $l > 2$ and $\widetilde{P}_K \subset G_L$ we must have that $I_K \subset G_L$. In other words, L/K is the degree 2 unramified extension and $\widetilde{\theta}_i$ both extend to G_L. In this case Proposition 43.6 implies
$$R^{\square}_{\overline{\rho}} \cong R^{\square}_{\rho_\theta}[[Z_1, Z_2, Z_3]]$$
where $\rho_\theta = \mathrm{Hom}_{\widetilde{P}_K}(\theta_1, \overline{\rho})$ is the one-dimensional G_L-representation.

Corollary 45.1. *(1) If θ_1 and θ_2 are not conjugate then*
$$R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[X_1, Y_1, X_2, Y_2, Z_1, Z_2]]/((1+Y_1)^{l^a} - 1, (1+Y_2)^{l^a} - 1)$$
for a equal to the l-adic valuation of $k^\times$ (recall k is the residue field of K).

(2) If θ_1 and θ_2 are conjugate then
$$R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[X, Y, Z_1, Z_2, Z_3]]/((1+Y)^{l^b} - 1)$$
for b equal the l-adic valuation of $l^\times$ for l/k the degree two extension.

46. Case of trivial prime to l-inertia

The only remaining possibility is that $\theta_1 = \theta_2 = \theta$. In this case we have $G_\theta = G_K$ so θ extends to a character of G_K. Using the isomorphism
$$R^{\square}_{\overline{\rho}} \cong R^{\square}_{\overline{\rho} \otimes \theta^{-1}}$$
we may assume that θ is the trivial character and so $\overline{\rho}|_{\widetilde{P}_K}$ is trivial. Proposition 43.3 shows that the same will be true for any deformation of $\overline{\rho}$. This reduces us to a computation of deformation rings for the group $T_K := G_K/\widetilde{P}_K$. As we've

seen previously this group has an explicit presentation: it fits into a split exact sequence

$$0 \to \mathbb{Z}_l \to T_K \to \widehat{Z} \to 0$$

and the quotient $\widehat{Z}$ acts on $\mathbb{Z}_l$ via conjugation by the l-adic cyclotomic character. Thus, if $\phi \in \widehat{Z}$ is the topological generator corresponding to arithmetic Frobenius and $\sigma \in \mathbb{Z}_l$ is a choice of topological generator then T_K is generated by σ and ϕ with the single relation

$$\phi\sigma\phi^{-1} = \sigma^q$$

for q equal the cardinality of k. By abuse of notation we write $I_K \subset T_K$ for the subgroup generated by σ.

Remark 46.1. This explicit presentation allows us to immediately give a description of $R^{\square}_{\overline{\rho}}$ in this case: let M denote the affine scheme over $\mathbb{Z}$ classifying 2×2-invertible matrices A and B which satisfy

$$ABA^{-1} = B^q$$

Then $\overline{\rho}$ corresponds to an $\mathbb{F}$-valued point of M and $R^{\square}_{\overline{\rho}}$ is the completion of the coordinate ring of M at the corresponding maximal ideal.

Lemma 46.2. *Let $\overline{\rho}$ be a two-dimensional $\mathbb{F}$-representation of T_K. Then $\overline{\rho}$ fits into an exact sequence*

$$0 \to \chi_1 \to \overline{\rho} \to \chi_2 \to 0$$

for χ_1, χ_2 unramified characters (i.e. characters with $\chi_i(\sigma) = 1$).

Proof. Since $I_K \subset T_L$ is an l-group there is a fixed vector $v \in \overline{\rho}|_{I_K}$. From the identity $\phi\sigma\phi^{-1} = \sigma^q$ we have

$$\overline{\rho}(\sigma)\overline{\rho}(\phi^{-1})v = \overline{\rho}(\phi^{-1})v$$

so $\overline{\rho}(\phi^{-1})v$ is also a fixed vector of $\overline{\rho}|_{I_K}$. Therefore, either $\overline{\rho}|_{I_K}$ is trivial or T_K stabilises the line generated by v. The lemma follows in either case. □

This lemma shows that (after possibly conjugating $\overline{\rho}$) we can write

$$\overline{\rho}(\sigma) = \begin{pmatrix} 1 & \overline{x} \\ 0 & 1 \end{pmatrix}, \qquad \overline{\rho}(\phi) = \begin{pmatrix} \overline{\alpha} & \overline{y} \\ 0 & \overline{\beta} \end{pmatrix}$$

for some $\overline{x}, \overline{y} \in \mathbb{F}$ and $\overline{\alpha}, \overline{\beta} \in \mathbb{F}^{\times}$.

Lemma 46.3. *Suppose $A \in \mathcal{C}$ and $\rho \in D^{\square}_{\overline{\rho}}(A)$. If $\overline{\alpha} \neq \overline{\beta}$ then there exists a unique $\left(\begin{smallmatrix} 1 & X \\ Y & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(A)$ such that*

$$\rho^{\mathrm{univ}}(\phi) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \Psi \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}$$

with Ψ diagonal.

Proof. The characteristic polynomial of $\rho(\phi)$ lifts $(X - \overline{\alpha})(X - \overline{\beta})$ and so by Hensel's lemma has two roots in A. Each of these roots is invertible in A and, since $\overline{\alpha} \neq \overline{\beta}$, their difference is also invertible. As a consequence there are eigenvectors $v_\alpha, v_\beta \in \rho$ for $\rho(\phi)$ forming a basis.

Let e_1, e_2 denote the standard basis on ρ. Then, scaling if necessary, we have $v_\alpha = e_1 + Xe_2$ and $v_\beta = Ye_1 + e_2$ for unique X, Y. This gives the lemma. □

Lemma 46.4. $\overline{\rho}(\sigma) = 1$ *unless* $\frac{\overline{\alpha}}{\overline{\beta}} \in \{1, q\}$.

Proof. We will have $\overline{\rho}(\sigma) = 1$ if the sequence $0 \to \chi_1 \to \overline{\rho} \to \chi_2 \to 0$ splits. In other words if the class of this extension in the Yoneda extension group $\mathrm{Ext}^1(\chi_2, \chi_1)$ is zero. Since

$$\mathrm{Ext}^1(\chi_2, \chi_1) = H^1(T_K, \mathrm{Hom}(\chi_2, \chi_1))$$

and $\mathrm{Hom}(\chi_2, \chi_1) \cong \chi_1/\chi_2$ it suffices to show $H^1(G_K, \chi_1/\chi_2) = 0$ when $\overline{\alpha}/\overline{\beta} \neq 1, q$. Using Tate's local Euler characteristic formula we have

$$\dim H^1(G_K, \chi_1/\chi_2) = \dim H^0(G_K, \chi_1/\chi_2) + \dim H^2(G_K, \chi_1/\chi_2)$$

Since χ_1/χ_2 is the unramified character sending ϕ onto $\overline{\alpha}/\overline{\beta}$ the H^0 vanishes except when $\overline{\alpha}/\overline{\beta} = 1$. Tate's local duality theorem says that $H^2(G_K, \chi_1/\chi_2) \cong H^0(G_K, \chi_{\mathrm{cyc}}\chi_2/\chi_1)$ for χ_{cyc} the mod l cyclotomic character. Since this is the unramified character sending ϕ onto $q\overline{\beta}/\overline{\alpha}$ it follows that the H^2 is zero except when $\overline{\alpha}/\overline{\beta} = q$. □

Corollary 46.5. *Suppose that* $\frac{\overline{\alpha}}{\overline{\beta}} \notin \{1, q\}$. *Then*

$$R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[A, B, P, Q, X, Y]]/((1+P)^{l^a} - 1, (1+Q)^{l^a} - 1)$$

and $\rho^{\mathrm{univ}}(\sigma)$ *is diagonal with eigenvalues* $1 + P$ *and* $1 + Q$.

Proof. For any $A \in \mathcal{C}$ and any $\rho \in D^{\square}_{\overline{\rho}}(A)$ the above implies there are uniquely determined $X, Y, A, B \in \mathfrak{m}_A$ so that

$$\rho(\phi) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha + A & 0 \\ 0 & \beta + B \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}$$

for fixed lifts α, β to $W(\mathbb{F})$ of $\overline{\alpha}, \overline{\beta}$. We also have that $P, Q, R, S \in \mathfrak{m}_A$ such that

$$\rho(\sigma) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1+P & R \\ S & 1+Q \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1},$$

The relation $\phi\sigma\phi^{-1} = \sigma^q$ implies

$$\begin{pmatrix} \alpha + A & 0 \\ 0 & \beta + B \end{pmatrix} \begin{pmatrix} 1+P & R \\ S & 1+Q \end{pmatrix} \begin{pmatrix} \alpha + A & 0 \\ 0 & \beta + B \end{pmatrix}^{-1} = \begin{pmatrix} 1+P & R \\ S & 1+Q \end{pmatrix}^q$$

Exercise 46.6. Looking at the off diagonal entries in this identity show that $R = S = 0$. Looking at the diagonal entries deduce that $(1+P)^q = (1+P)$ and that $(1+Q)^q = (1+Q)$, and therefore that $(1+P)^{l^a} = 1$ and $(1+Q)^{l^a} = 1$.

Conversely, given X, Y, A, B, P, Q the given formula for $\rho(\sigma)$ and $\rho(\phi)$ define a deformation of $\overline{\rho}$. This proves that $R^{\square}_{\overline{\rho}}$ is as claimed. □

One can also address some situations where $\overline{\alpha}/\overline{\beta} \in \{1, q\}$. For example:

Proposition 46.7. *(1) Suppose that*

$$\overline{\rho}(\sigma) = 1, \qquad \overline{\rho}(\psi) = \begin{pmatrix} 1 & \overline{y} \\ 0 & 1 \end{pmatrix}$$

If $q \not\equiv 1$ modulo l then $R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[P, Q, R, S]]$.

(2) Suppose that

$$\overline{\rho}(\sigma) = \begin{pmatrix} 1 & \overline{x} \\ 0 & 1 \end{pmatrix}, \qquad \overline{\rho}(\psi) = \begin{pmatrix} q & \overline{y} \\ 0 & 1 \end{pmatrix}$$

If $q \not\equiv \pm 1$ modulo l then either

(a) $\overline{x} \neq 0$ and $R^{\square}_{\overline{\rho}}$ is formally smooth over $W(\mathbb{F})$.

(b) $\overline{x} = 0$ and $R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[X_1, \ldots, X_5]]/(X_1 X_2)$.

Proof. First, lets do (1). Write

$$\rho^{\mathrm{univ}}(\sigma) = \begin{pmatrix} 1 + A & B \\ C & 1 + D \end{pmatrix}, \qquad \rho^{\mathrm{univ}}(\phi) = \begin{pmatrix} 1 + P & y + R \\ S & 1 + Q \end{pmatrix}$$

for some $y \in W(\mathbb{F})$ lifting $\overline{y}$. Set $I = (A, B, C, D)$ and consider the equation $\rho^{\mathrm{univ}}(\phi)\rho^{\mathrm{univ}}(\sigma) = \rho^{\mathrm{univ}}(\sigma)^q \rho^{\mathrm{univ}}(\phi)$ modulo the ideal $I\mathfrak{m}$. Looking at the four entries gives four congruences

$$yC \equiv (q-1)A, \qquad B + Dy \equiv qAy + qB$$
$$C \equiv qC, \qquad (q-1)D + qCy$$

all modulo $I\mathfrak{m}$. Since $q \neq 1$ it follows that $I \subset I\mathfrak{m}$ and Nakayama's lemma therefore implies $I = 0$. We conclude that ρ^{univ} is unramified and so $R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[P, Q, R, S]]$.

Part (2) is similar. Since $q \neq 1$ we can write

$$\rho^{\mathrm{univ}}(\sigma) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 + A & x + B \\ C & 1 + D \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}, \qquad \rho^{\mathrm{univ}}(\phi) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} q(1+P) & \\ & 1 + Q \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}$$

for $x \in W(\mathbb{F})$ a lift of $\overline{x}$. A similar argument as before with $I = (A, C, D)$ and using that $q^2 \neq 1$ shows that $A = C = D = 0$. Then looking directly at the identity $\rho^{\mathrm{univ}}(\phi)\rho^{\mathrm{univ}}(\sigma) = \rho^{\mathrm{univ}}(\sigma)^q \rho^{\mathrm{univ}}(\phi)$ (not modulo any ideal) one finds that

$$(x + B)(P - Q) = 0$$

We therefore obtain a surjective map $W(\mathbb{F})[[B, P, Q, X, Y]]/((x - B)(P - Q)) \to R^{\square}_{\overline{\rho}}$. One check that the above formula's for $\rho^{\mathrm{univ}}(\sigma)$ and $\rho^{\mathrm{univ}}(\psi)$ define a representation on $W(\mathbb{F})[[B, P, Q, X, Y]]/((x - B)(P - Q))$ and so this map is an isomorphism. If $\overline{x} \neq 0$ then we must have $P = Q$ and so

$$R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[X_1, \ldots, X_4]]$$

If $\overline{x} = 0$ then
$$R^{\square}_{\overline{\rho}} \cong W(\mathbb{F})[[B, P, U, X, Y]]/(BU)$$
where we've set $U = P - Q$. □

The remaining cases are more complicated so we won't give direct calculations in these cases.

Lecture 22

47. Reduction modulo p

The goal here is to describe some basic results around the process of "reducing" a representation $\rho : G \to \mathrm{GL}_n(E)$ modulo p for E a finite extension of $\mathbb{Q}_p$ and G a profinite group. Write V for representation of G on the vector space E^n induced by ρ.

Definition 47.1. Let $\mathcal{O}$ denote the ring of integers inside E. A lattice $T \subset V$ is an $\mathcal{O}$-submodule of V such that the following equivalent conditions hold:

(1) T is finitely generated over $\mathcal{O}$ and T generates V over E.
(2) T is finitely generated over $\mathcal{O}$ and the map $T \otimes_{\mathcal{O}} K \to V$ given by $t \otimes x \mapsto xt$ is an isomorphism.
(3) T is a free $\mathcal{O}$-module of rank d.

The equivalence of these three conditions comes down to the observation that $T \otimes_{\mathcal{O}} K \to V$ is injective for any $\mathcal{O}$-submodule $T \subset V$. Indeed, if $\sum v_i t_i = 0$ for $v_i \in K$ and $t_i \in T$ then choose n so that $\pi^n v_i \in \mathcal{O}$ for all n with $\pi \in K$ a uniformiser. One has

$$\sum t_i \otimes v_i = \sum t_i \otimes (\pi^n v_i)\pi^{-n} = \sum \left((t_i \pi^n v_i) \otimes \pi^{-n}\right) = \left(\sum t_i \pi^n v_i\right) \otimes \pi^{-n} = 0$$

Lemma 47.2. *If $T_1, T_2 \subset V$ are lattices then so is $T_1 + T_2$.*

Proof. This is clear from condition (1) in the above definition. □

Lemma 47.3. *There always exists a lattice $T \subset V$ such that T is stable under the action of G. Equivalently, there exists $K \in \mathrm{GL}_n(E)$ such that $K\rho(g)K^{-1} \in \mathrm{GL}_n(\mathcal{O})$ for every $g \in G$.*

Proof. Choose a lattice $T' \subset V$ (for example take $\mathcal{O}^n \subset E^n$). Then $H = \{g \in G \mid gT \subset T\}$ is an open subgroup of G (because $\mathrm{GL}_n(\mathcal{O}) \subset \mathrm{GL}_n(E)$ is an open subgroup). Thus, G/H is finite and so we can consider

$$T = \sum_{g \in G/H} gT$$

which is again a lattice in V and which is stable under the action of G. □

This gives us a way of reducing ρ modulo p. We can choose a stable lattice $T \subset V$ and define the reduction modulo p as $T \otimes_{\mathcal{O}} \mathbb{F}$ (here $\mathbb{F}$ is the residue field of $\mathcal{O}$). Equivalently, choose K so that $K\rho(g)K^{-1} \in \mathrm{GL}_n(\mathcal{O})$ and define the $\overline{\rho} : G \to \mathrm{GL}_n(\mathbb{F})$ by sending g onto the image of $K\rho(g)K^{-1}$ under

$$\mathrm{GL}_n(\mathcal{O}) \to \mathrm{GL}_n(\mathbb{F})$$

Of course this definition has a problem because the may be many different choices of stable lattice in V (equivalently there may be many different K's such that $K\rho(g)K^{-} \in \mathrm{GL}_n(\mathcal{O})$ for all $g \in G$. Here is one situation where this is not a problem:

Lemma 47.4. *Suppose that for some choice of stable lattice $T \subset V$ the representation $T \otimes_{\mathcal{O}} \mathbb{F}$ is irreducible. Then any other stable lattice $T' \subset V$ is a scalar multiple of T (i.e. $T' = xT$ for some $x \in K$). In particular, $T \otimes_{\mathcal{O}} \mathbb{F} \cong T' \otimes_{\mathcal{O}} \mathbb{F}$ so the reduction modulo p is well defined.*

Proof. Let T' be another stable lattice. Replacing T' by $\pi^n T'$ for n sufficiently large we can suppose that $T' \subsetneq T$. If $T' \neq T$ then the image of the map

$$T' \to T \times_{\mathcal{O}} \mathbb{F}$$

is a proper stable subspace inside $T \otimes_{\mathcal{O}} \mathbb{F}$ and so, since $T \otimes_{\mathcal{O}} \mathbb{F}$ is assumed irreducible, must be zero. Therefore either $T' = T$ or $T' \subset \pi T$ for $\pi \in E$ a uniformiser, and so $\pi^{-1} T' \subset T$. In the second case, repeating the argument shows that either $\pi^{-1} T' = T$ or $\pi^{-2} T' \subset T$. Continuing in this way we deduce that either $\pi^{-n} T' = T$ for some $n \geq 0$ or $\pi^{-n} T' \subset T$ for every $n \geq 0$. The second possibility is impossible so T' is a scaler multiple of T. □

On the other hand, things can go wrong when $T \otimes_{\mathcal{O}} \mathbb{F}$ is not irreducible.

Example 47.5. Consider a representation $\rho : G \to \mathrm{GL}_2(\mathcal{O})$ with

$$\rho(g) = \begin{pmatrix} \chi(g) & 0 \\ 0 & 1 \end{pmatrix}$$

for χ a character. Write $T = \mathcal{O}^2$ for the corresponding representation. Now suppose that $\chi \equiv 1$ modulo π. Then for $K = \left(\begin{smallmatrix} 1 & \pi^{-1} \\ 0 & 1 \end{smallmatrix}\right)$ we have

$$K^{-1} \rho(g) K = \begin{pmatrix} \chi(g) & \pi^{-1}(\chi(g) - 1) \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{O})$$

for every $g \in G$. This K corresponds to another choice of stable lattice T' inside $V = T[\frac{1}{p}]$. If $\chi \not\equiv 1$ modulo π^2 then $T' \otimes_{\mathcal{O}} \mathbb{F}$ and $T \otimes_{\mathcal{O}} \mathbb{F}$ are not isomorphic (because one is trivial and one is not).

48. Cohomological interpretation of the previous example

The goal here is to give an idea of how you could come up with the previous example by thinking in terms of cohomology. For this we need to think about cohomology groups $H^i(G, V)$ for V a representation of G on either an E-vector space or a finitely generated (but not necessarily set-finite) $\mathcal{O}$-module. Note the usual set-up for group cohomology does not apply here since such V are not discrete G-modules. To fix this we make a "naive" definition by setting

$$H^0_{\mathrm{cont}}(G, V) = V^G$$

and

$$H^1_{\mathrm{cont}}(G, V) = \{\text{continuous 1-cocycles } G \to V\} / \{\text{1-coboundaries}\}$$

We need the following properties of these groups:

(1) If $0 \to V_1 \to V \to V_2 \to 0$ is an exact sequence then there is the usual associated long exact sequence

$$0 \to H^0(G, V_1) \to H^0(G, V) \to H^0(G, V_2) \to H^1(G, V_1) \to H^1(G, V) \to H^1(G, V_2)$$

(2) Assume V is a finitely generated $\mathcal{O}$-module. Then the obvious map $H^1(G,V) \to H^1(G, V \otimes_{\mathcal{O}} \mathbb{F})$ induces an identification $H^1(G,V) \otimes_{\mathcal{O}} \mathbb{F} \cong H^1(G, V \otimes_{\mathcal{O}} \mathbb{F})$ and likewise with $\mathbb{F}$ replaced by E.

(3) Now assume V is a finite free $\mathcal{O}$-module or a finite dimensional E-vector space. Then, in the usual way we can identify $H^1(G,V) = \operatorname{Ext}^1(1,V)$ and, if V is a finite free $\mathcal{O}$-module, then under these identifications the maps

$$H^1(G, V \otimes_{\mathcal{O}} \mathbb{F}) \leftarrow H^1(G,V) \to H^1(G, V \otimes_{\mathcal{O}} E)$$

corresponds to the maps on extension groups obtained by applying $\otimes_{\mathcal{O}}\mathbb{F}$ and $\otimes_{\mathcal{O}}E$.

Point (3) shows that one can find stable lattices inside $V[\frac{1}{p}] \otimes 1$ by considering classes in $H^1(G,V)$ whose image in $H^1(G, V[\frac{1}{p}])$ is zero. Point (2) shows that these are precisely the torsion classes in $H^1(G,V)$ and the π^n-torsion inside $H^1(G,V)$ can be accessed using point (1). From the exact sequence $0 \to V \xrightarrow{\pi^n} V \to V/\pi^n V \to 0$ we obtain an exact sequence

$$H^0(G,V) \to H^0(G, V/\pi^n V) \to H^1(G,V) \xrightarrow{\pi^n} H^1(G,V)$$

Therefore, the π^n-torsion is given by the image of the boundary map $H^0(G, V/\pi^n V) \to H^1(G,V)$. Concretely this map sends a fixed element $\overline{v} \in V/\pi^n V$ onto the 1-cocycle

$$\sigma \mapsto \frac{\sigma(v) - v}{\pi^n}$$

for $v \in V$ and lift of $\overline{v}$. If $H^0(G,V) = 0$ then this map is injective

49. Reduction modulo p and Grothendieck groups

To obtain a well defined notion of reduction modulo p one needs to pass to Grothendieck groups.

Definition 49.1. Let $\mathbb{F}$ be any field (i.e. possibly a finite field or a finite extension of $\mathbb{Q}_p$) and let $\operatorname{Rep}_{\mathbb{F}}(G)$ denote the category of continuous $\mathbb{F}$-representation of a profinite group G. Then the Grothendieck group $K_0(\operatorname{Rep}_{\mathbb{F}}(G))$ is the quotient of the free abelian group generated by $[V]$ for $V \in \operatorname{Rep}_{\mathbb{F}}(G)$ by the relations

$$[V] = [V_1] + [V_2]$$

whenever $0 \to V_1 \to V \to V_2 \to 0$ is an exact sequence.

Lemma 49.2. *Choose a set of representatives of the isomorphism classes of irreducible representations in* $\operatorname{Rep}_{\mathbb{F}}(G)$. *Then every element of* $K_0(\operatorname{Rep}_{\mathbb{F}}(G))$ *can be written runs uniquely as*

$$\sum_V n_V [V]$$

where V runs over a finite set of these representatives and $n_V \in \mathbb{Z}$.

By the same construction one can form the Grothendieck group of any category in which exact sequences make sense. For example, it can be formed for any abelian category.

Lemma 49.3. *Suppose that*

$$0 \to V_1 \to \dots \to \dots \to V_n \to 0$$

is a long exact sequence in $\mathrm{Rep}_{\mathbb{F}}(G)$*. Then*

$$\sum (-1)^i [V_i] = 0$$

in $K_0(\mathrm{Rep}_{\mathbb{F}}(G))$*.*

Proof. If $n = 3$ this is by definition and for general $n > 3$ one argues by induction by considering the exact sequences

$$0 \to V_1 \to \dots V_{n-3} \xrightarrow{f} V_{n-2} \to \operatorname{im} f \to 0$$

and

$$0 \to \operatorname{im} f \to V_{n-1} \to V_n \to 0$$

By induction the first sequence gives $\sum_{i=1}^{n-2} (-1)^i [V_i] + (-1)^{n-1} [\operatorname{im} f] = 0$ and the second sequence gives $(-1)^{n-1}[\mathrm{imf}(f)] = (-1)^{n-1}[V_{n-1}] + (-1)^n [V_n]$. □

Proposition 49.4. *Suppose E is a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}$ then there is a homomorphism*

$$\mathrm{red} : K_0(\mathrm{Rep}_E(G)) \to K_0(\mathrm{Rep}_{\mathbb{F}}(G))$$

such that $\mathrm{red}([V]) = [T \otimes_{\mathcal{O}} \mathbb{F}]$ *for any stable lattice $T \subset V$.*

Proof. First note that if the class $[T \otimes_{\mathcal{O}} \mathbb{F}]$ in $K_0(\mathrm{Rep}_{\mathbb{F}}(G))$ is independent of the choice of stable lattice $T \subset V$ then the map this formula defines is a homomorphism because if $0 \to V_1 \to V \to V_2 \to 0$ is an exact sequence then

$$0 \to T \cap V_1 \to T \to \operatorname{im} T \to 0$$

is an exact sequence of flat (i.e. torsionfree) $\mathcal{O}$-modules and so the exact sequence

$$0 \to (T \cap V_1) \otimes_{\mathcal{O}} \mathbb{F} \to T \otimes_{\mathcal{O}} \mathbb{F} \to \operatorname{im} T \otimes_{\mathcal{O}} \mathbb{F} \to 0$$

witnesses the identity $\mathrm{red}([V]) = \mathrm{red}([V_1]) + \mathrm{red}([V_2])$.

Therefore to finish the proof suppose T' and T are stable lattices in V. First assume $\pi T \subset T' \subset T$. In this case there is an exact sequence

$$0 \to T/T' \xrightarrow{\pi} T' \otimes_{\mathcal{O}} \mathbb{F} \to T \otimes_{\mathcal{O}} \mathbb{F} \to T/T' \to 0$$

which shows that $[T' \otimes_{\mathcal{O}} \mathbb{F}] = [T \otimes_{\mathcal{O}} \mathbb{F}]$. For the general case, we can multiply T' by a scalar (since this does not change the isomorphism class of $T' \otimes_{\mathcal{O}} \mathbb{F}$) and assume $\pi^n T \subset T' \subset T$ for some $1 \geq 0$. We've just treated the case $n = 1$ and for $n > 1$ we argue by induction as follows. Set $T'' = \pi^{n-1} T + T'$. Then

$$\pi^{n-1} T \subset T'' \subset T, \qquad \pi T'' \subset T' \subset T''$$

and so $[T \otimes_{\mathcal{O}} \mathbb{F}] = [T'' \otimes_{\mathcal{O}} \mathbb{F}] = [T' \otimes_{\mathcal{O}} \mathbb{F}]$. □

Corollary 49.5. *Let*

$$0 = F_n \subset F_{n-1} \subset \ldots \subset F_1 \subset F_0 = T \otimes_{\mathcal{O}} \mathbb{F}$$

be a composition series of $T \otimes_{\mathcal{O}} \mathbb{F}$, i.e. a sequence of stable subspaces whose subquotients are all irreducible. Define the semi-simplification

$$(T \otimes_{\mathcal{O}} \mathbb{F})^{\mathrm{ss}} := \bigoplus_i F_i / F_{i+1}$$

Then $(T \otimes_{\mathcal{O}} \mathbb{F})^{\mathrm{ss}}$ is (up to isomorphism) independent of the choice of composition series and the choice of stable lattice $T \subset V$.

50. Aside—Ribet's Lemma

Let us finish with an interesting result regarding reduction modulo p. We probably won't use this in the future but its something good to know.

Proposition 50.1 (Ribet's Lemma)**.** *Let G be a profinite group (even just compact) and suppose that $\rho : G \to \mathrm{GL}_2(E)$ is a continuous irreducible representation for which $\overline{\rho}^{\mathrm{ss}} = \chi_1 \oplus \chi_2$ with χ_1 and χ_2 one dimensional. Then there exists a stable lattice T inside V such that $T \otimes_{\mathcal{O}} \mathbb{F}$ is a non-split extension of χ_1 by χ_2.*

Below we give a sketch of one possible proof of this result using the tree attached to PGL_2: Let X denote the set of homothety classes of lattices inside E^2. We can make X into an undirected graph by asserting that $[V], [V'] \in X$ are connected if $\pi V \subset V' \subset V$ or vice versa.

Lemma 50.2. *X is simply connected, in other words any two points are connected by a unique path.*

Let $C \subset X$ denote the set of vertices which are stable under the action of G via ρ. Then one has

Lemma 50.3. *C is non-empty and convex (i.e. every point on the unique path between two points in C must also be in C).*

Proof. This is because each $g \in G$ sends a path between two points in C onto another such path; by uniqueness this must be the path we started with. □

Lemma 50.4. *Suppose $x \in C$ and let $\overline{\rho}_x$ be the reduction of the corresponding stable lattice. Then*

(1) $\overline{\rho}_x$ is irreducible if and only if C consists of a single point.
(2) $\overline{\rho}_x$ is a non-split extension of two one characters if and only if every $x \in C$ has exactly one neighbour.
(3) $\overline{\rho}_x$ is a split extension of two characters if it has > 1 neighbour. If the characters are distinct then it will have exactly two neighbours.

The last ingredient is then:

Lemma 50.5. *If ρ is irreducible if and only if C is bounded, i.e. each path has finite length.*

Lecture 23

51. Grothendieck's l-adic monodromy theorem

In the following section let $K/\mathbb{Q}_p$ be a finite extension and let E be a finite extension of $\mathbb{Q}_l$ with $l \neq p$. Consider a continuous representation $\rho : G_K \to \mathrm{GL}_n(E)$. Write $V = E^n$ for the vector space on which G_K acts via ρ.

Recall $I_K \subset G_K$ is the inertia subgroup and $I_K/\widetilde{P}_K$ is the maximal pro-l-quotient.

Lemma 51.1 (Grothendieck)**.** *$\rho(\widetilde{P}_K)$ is a finite group.*

Proof. Replace ρ by a conjugate so that $\rho(G_K) \subset \mathrm{GL}_n(\mathcal{O})$ for $\mathcal{O} \subset E$ the ring of integers (equivalently, choose a stable lattice). Since $\rho(\widetilde{P}_K)$ is a closed prime-to-l order subgroup of $\mathrm{GL}_n(\mathcal{O})$ it intersects the kernel of

$$\mathrm{GL}_n(\mathcal{O}) \to \mathrm{GL}_n(\mathbb{F})$$

trivially (since this kernel is pro-l). Therefore $\rho(\widetilde{P}_K)$ injects into $\mathrm{GL}_n(\mathbb{F})$ and so is finite. □

Corollary 51.2 (Grothendieck)**.** *There exists an open subgroup $I_1 \subset I_K$ such that $\rho(g)$ is unipotent for all $g \in I_1$.*

Proof. Replacing K by a finite extension we can assume that $\rho(\widetilde{P}_K) = 1$. Then ρ is a representation of the group $T_K = G_K/\widetilde{P}_K$. Recall this group can be generated by σ, ϕ with $\sigma \in I_K/\widetilde{P}_K$ and the relation

$$\phi\sigma\phi^{-1} = \sigma^q$$

Therefore, if $v \in V$ has $\sigma v = av$ for $a \in E$ then

$$\sigma(\phi^{-1}v) = a^q\phi^{-1}v$$

Therefore, if a is an eigenvalue of $\rho(\sigma)$ then so is a^q. It follows that each a is a root of unity and so, for sufficiently large N, every eigenvalue of $\rho(\sigma^N)$ is 1. Therefore we can take $I_1 \subset I_K$ equal to the subgroup corresponding to that generated by σ^N in $I_K/\widetilde{P}_K$. □

The next step is where we use that the coefficients of ρ have characteristic zero. This means that at any unipotent endomorphism U (i.e. $U - 1$ is nilpotent) of V can be written as

$$\exp(N)$$

for $N = \log(U)$ which is a nilpotent matrix .

Proposition 51.3. *There exists an open subgroup $I_1 \subset I_K$ and nilpotent endomorphism N of V such that*

$$\rho(g) = \exp(t(g)N)$$

for every $g \in I_1$. Here $t : I_K \to \mathbb{Z}_l$ is the map induced by the isomorphism $I_K/\widetilde{P}_K \cong \mathbb{Z}_l$.

Proof. Choose $x \in I_1$ with $t(x) = 1$ and which topologically generates $\rho(I_1)$. Then we can write $\rho(x) = \exp(N)$ for a nilpotent matrix N. For any $g \in I_1$ we have

$$\rho(g) = \rho(x^r) = \exp(N)^r = \exp(rN)$$

for some $r \in \mathbb{Z}_l$. We just need to show that $r = t(g)$ and this follows because $\rho(\widetilde{P}_K \cap I_1) = 1$ by construction so that $\rho|_{I_1}$ factors through the $t|_{I_1} : I_1 \to \mathbb{Z}_l$. □

52. Weil–Deligne representations

Keep the notation from the previous section. We are going to show how the previous proposition allows us to relate ρ to a representation of the Weil group:

Definition 52.1. Let $W_K \subset G_K$ denote the subgroup generated by I_K and the preimage under $G_K \to G_k$ of the subgroup generated (not topologically generated) by the Frobenius ϕ in G_k Thus W_K sits in an exact sequence

$$0 \to I_K \to W_K \to \mathbb{Z} \to 0$$

Equip W_K with the topology defined so that $I_K \subset W_K$ has the profinite topology and $W_K \to \mathbb{Z}$ is continuous. Note this is not the subspace topology coming from G_K because $I_K \subset W_K$ is open.

Definition 52.2. A Weil–Deligne representation of W_K is a pair (ρ', N) where

- $\rho' : W_K \to \mathrm{GL}_n(E)$ is a continuous representation for the discrete topology on $\mathrm{GL}_n(E)$. This is the same as asking that $\rho'(I_K)$ is finite.
- N is a nilpotent matrix satisfying

$$\rho'(g)N\rho'(g)^{-1} = \chi(g)N$$

for every $g \in W_K$, where χ is the l-adic cyclotomic character.

Note that in the definition of a Weil–Deligne representation the topology on the field E is not important.

Proposition 52.3. *A Weil–Deligne representation (ρ', N) can be attached to ρ so that*

$$\rho(\phi^n g) = \rho'(\phi^n g)\exp(t(g)N)$$

for any $g \in I_K$ and any lift of Frobenius F.

Proof. Let N be the nilpotent matrix attached to ρ from before, and define $\rho' : W_K \to \mathrm{GL}_n(E)$ by setting

$$\rho'(\phi^n g) = \rho(\phi^n g)\exp(-t(g)N)$$

By construction $\rho'(I_K)$ is finite so ρ' is continuous when $\mathrm{GL}_n(E)$ has the discrete topology. Using that $\rho(\phi)\exp(N)\rho(\phi)^{-1} = \exp(qN)$ one checks that ρ' is also a homomorphism and that N satisfies the relation required to be a Weil–Deligne representation. □

In the two dimensional case we have

Lemma 52.4. *Suppose that $n = 2$ and that $N \neq 0$. Then*

$$\rho'(g) = \begin{pmatrix} \gamma(g)\chi(g) & * \\ 0 & \gamma(g) \end{pmatrix}$$

for some character γ. Similarly for ρ.

Proof. Note that the identity $\rho'(g)N\rho'(g)^{-1} = \chi(g)N$ implies that $\ker N$ is stable under ρ'. Therefore, if $\ker N \neq 0$ then in the two dimensional case it follows that ρ' is reducible. Conjugating we can assume that $N = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and that

$$\rho'(g) = \begin{pmatrix} \gamma_1(g) & * \\ 0 & \gamma_2(g) \end{pmatrix}$$

Since

$$\rho'(g)N\rho'(g)^{-1} = \begin{pmatrix} 0 & \gamma_1(g)\gamma_2(g)^{-1} \\ 0 & 0 \end{pmatrix}$$

it follows that $\gamma_1 = \gamma_2\chi$. □

53. Weil–Deligne representations over deformation rings

Now we return to the setting of a deformation ring. Let K and E be as above and let $\mathcal{O}$ be the ring of integers in E with residue field $\mathbb{F}$. Fix $\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$ and let $R^{\square}_{\overline{\rho}}$ be the framed deformation ring with universal deformation ρ^{univ}.

Proposition 53.1. *Write $\rho^{\mathrm{univ}} : G_K \to \mathrm{GL}_n(R^{\square}_{\overline{\rho}}[\frac{1}{l}])$. Then there exists a nilpotent $N \in \mathrm{Mat}_n(R^{\square}_{\overline{\rho}}[\frac{1}{l}])$ such that*

$$\rho^{\mathrm{univ}}(g) = \exp(t(g)N)$$

for all $g \in I_1 \subset I_K$ some open subgroup. We can associate to ρ^{univ} the pair $(\rho^{\mathrm{univ}\prime}, N)$ where $\rho^{\mathrm{univ}\prime} : G_K \to \mathrm{GL}_n(R^{\square}_{\overline{\rho}}[\frac{1}{l}])$ is defined by

$$\rho^{\mathrm{univ}\prime}(\phi^n g) = \rho^{\mathrm{univ}}(\phi^n g)\exp(-t(g)N)$$

for $g \in I_K$ and $\rho^{\mathrm{univ}\prime}(I_K)$ is a finite group.

Exercise 53.2. Prove this using the same strategy as in the case of a field.

Recall that an irreducible component of $\mathrm{Spec}\, R^{\square}_{\overline{\rho}}[\frac{1}{l}]$ is a maximal irreducible closed subscheme. These are in bijection with minimal primes of $R^{\square}_{\overline{\rho}}[\frac{1}{l}]$ via the correspondence

$$\mathfrak{p} \mapsto \mathrm{Spec}\, R^{\square}_{\overline{\rho}}[\frac{1}{l}]/\mathfrak{p}$$

Lemma 53.3. *Assume that R is a p-torsionfree $\mathbb{Z}_p$-algebra. Then the irreducible components of $\mathrm{Spec}\, R$ are in bijection with the irreducible components of $\mathrm{Spec}\, R[\frac{1}{l}]$.*

Proof. Recall that for any multiplicative subset $S \subset R$ the set of prime ideals in $S^{-1}R$ are in bijection with those prime ideals in R which do not intersect S. This bijection sends $\mathfrak{p} \subset S^{-1}R$ onto the preimage of $\mathfrak{p}$ under the natural map $R \to S^{-1}R$, and in particular is order preserving. Therefore, it suffices to show that every minimal prime in R does not contain p.

Suppose one minimal prime of R contains p. If $\mathfrak{q} \subset R$ does not contain p then $R/\mathfrak{q}$ is also p-torsionfree. Therefore, we can reduce to the case where every minimal prime of R contains p. Then p is contained in the intersection of all minimal primes and this is the nilradical of R (i.e. the set of nilpotent elements). It follows that p is nilpotent which contradicts the assumption that R is p-torsionfree. □

Corollary 53.4. *Let $x, y : R^{\square}_{\overline{\rho}} \to \overline{E}$ be two homomorphisms and write ρ_x, ρ_y for the representations $G_K \to \mathrm{GL}_n(\overline{E})$ obtained by specialising ρ^{univ}. Assume that both x and y factor through $R^{\square}_{\overline{\rho}}/\mathfrak{p}$ for $\mathfrak{p}$ a minimal prime. Then*

$$\rho'_x|_{I_K} \cong \rho'_y|_{I_K}$$

Note here that

Proof. Set $C = R^{\square}_{\overline{\rho}}[\frac{1}{l}]$ and write $\rho'_C : G_K \to \mathrm{GL}_n(C)$ for the specialisation of $\rho^{\mathrm{univ}'}$ to C. Let I_1 be as in the proposition so that $\rho'_C(I_1) = 1$ and consider the characteristic polynomial $P(\rho'_C, g) \in C[T]$ for every $g \in I_K/I_1$. Choose representatives $\eta_1, \dots, \eta_j$ of isomorphism classes of representations of I_K/I_1. Then for each $i = 1, \dots, j$ we can consider the closed subscheme $Z_i \subset \operatorname{Spec} C$ defined by the condition that

$$P(\rho'_C, g) = P(\eta_i, g)$$

where $P(\eta_i, g)$ denotes the characteristic polynomial of $\eta_i(g)$. Concretely, Z_i corresponds to the ideal of C generated by the coefficients of $P(\rho'_C, g) = P(\eta_i, g)$. Then

$$\operatorname{Spec} C = \bigcup_{i=1}^{j} Z_i$$

Since $\operatorname{Spec} C$ is irreducible and this is a finite union we must have $\operatorname{Spec} C = Z_i$ for some i. Writing $P(\rho'_x, g)$ for the characteristic polynomial of $\rho'_x(g)$ and likewise for ρ'_y we get that

$$P(\rho'_x, g) = P(\rho'_y, g)$$

for every $g \in I_K$. Since these are representations on an algebraically closed field of characteristic zero it follows that $\rho'_x|_{I_K} \cong \rho'_y|_{I_K}$. □

This shows that over $\operatorname{Spec} R^{\square}_{\overline{\rho}}[\frac{1}{l}]$ the ρ' part of the Weil–Deligne representations remains constant on each irreducible component. However the N part can vary.

Part 2. Lecture 24

54. Inertial types

As usual $K/\mathbb{Q}_p$ is a finite extension and $E/\mathbb{Q}_l$ is another finite extension with $l \neq p$. Let $\mathcal{O}$ denote the ring of integers in E and $\mathbb{F}$ the residue field of E. Fix

$\overline{\rho} : G_K \to \mathrm{GL}_n(\mathbb{F})$. Rather than consider the usual deformation ring of $\overline{\rho}$ we consider its base-change

$$R^{\square} := R^{\square}_{\overline{\rho}} \otimes_{W(\mathbb{F})} \mathcal{O}$$

Recall from last lecture the definition of a Weil–Deligne representation:

Definition 54.1. A Weil–Deligne representation of W_K is a pair (ρ', N) where

- $\rho' : W_K \to \mathrm{GL}_n(E)$ is a continuous representation for the discrete topology on $\mathrm{GL}_n(E)$. This is the same as asking that $\rho'(I_K)$ is finite.
- N is a nilpotent matrix satisfying
$$\rho'(g) N \rho'(g)^{-1} = \chi(g) N$$
for every $g \in W_K$, where χ is the l-adic cyclotomic character.

We saw last time how to attach a Weil–Deligne representation (ρ', N) to any l-adic representation $\rho : G_K \to \mathrm{GL}_n(E)$. We also saw that if $\mathcal{C} \to \operatorname{Spec} R^{\square}[\frac{1}{l}]$ was a (geometrically) irreducible closed subscheme and $\rho_x, \rho_y : G_K \to \mathrm{GL}_n(E)$ are representations corresponding to morphisms $x, y : \operatorname{Spec} R \to \mathcal{C}$ then

$$\rho'_x|_{I_K} \cong \rho'_y|_{I_K}$$

where (ρ'_x, N_x) and (ρ'_y, N_y) are the corresponding Weil–Deligne representations. This motivates the following definition

Definition 54.2. An inertial type is an equivalence class of pairs (r_τ, N_τ) with

- $r_\tau : I_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_l)$ a representation
- N_τ is a nilpotent matrix
- (r_τ, N_τ) extends to a Weil–Deligne representation.

In particular this implies that r_τ has finite image and that N_τ commutes with the image of r_τ.

Proposition 54.3. *Assume that τ is an inertial type which is defined over E (so $r_\tau(x)$ and N_τ are matrices over E for all $x \in I_K$). Then there exists a quotient $R^{\square}(\tau)$ of $R^{\square}$ with the following property: any map $x : R^{\square} \to E'$ with E'/E a finite extension factors through $R^{\square}(\tau)$ if and only if the corresponding representation ρ_x has Weil–Deligne representation (ρ'_x, N_x) with*

$$\rho'_x|_{I_K} \cong r_\tau, N_x = N_\tau$$

Furthermore, this condition uniquely determines $R^{\square}(\tau)$ if we also ask that $R^{\square}(\tau)$ be reduced and p-torsionfree.

Proof. Recall that we can attach a universal Weil–Deligne representation $(\rho\mathrm{univ}', N^{\mathrm{univ}})$ to $\rho^{\mathrm{univ}} : G_K \to \mathrm{GL}_n(R^{\square}[\frac{1}{l}])$ so that (ρ'_x, N_x) is obtained by specialising $(\rho\mathrm{univ}', N^{\mathrm{univ}})$ along $x : R^{\square} \to E'$. Consider the ideal $I \subset R^{\square}[\frac{1}{l}]$ generated by

$$r_\tau(x)_{ij} - \rho^{\mathrm{univ}'}(x)_{ij}, \qquad N^{\mathrm{univ}}_{ij} - N_{\tau,ij}$$

for all $x \in I_K$. Then

$$\rho'_x|_{I_K} \cong r_\tau, N_x = N_\tau$$

if and only if x factors through $R^{\square}[\frac{1}{l}]/I$.

Remark 54.4. Note this condition does not determine I uniquely, it only determines a closed subset inside $|\operatorname{Spec} R^\square[\frac{1}{l}]|$. But such a closed subscheme can be given many different scheme structures.

We can take $R^\square(\tau)$ and quotient of $R^\square$ so that $R^\square(\tau)[\frac{1}{l}] = R^\square[\frac{1}{l}]/I$. For example, we could take $R^\square(\tau) = R^\square/I'$ where I' is the preimage of I under $R^\square \to R^\square[\frac{1}{l}]$.

Note that it $R^\square/I_1$ and $R^\square/I_2$ are two such quotients satisfying the conditions in the proposition then so does $R^\square/I_1 \cap I_2$. Therefore, there is a minimal ideal $I_{\min}$ such that $R^\square/I_{\min}$ is as required. This must be a radical ideal and cannot contain any power of p . Thus $R^\square/I$ reduced and p-torsionfree. □

Definition 54.5. From now on, when we write $R^\square(\tau)$ we require that it be reduced and p-torsionfree. Thus, this quotient of $R^\square$ is uniquely determined.

We would like to understand $\overline{R}^\square(\tau) = R^\square(\tau) \otimes_{\mathcal{O}} \mathbb{F}$. Note that with the previous definition it is not completely clear how to do this. If one wants to understand $\overline{R}^\square_\tau$ one would like to understand which morphisms $R^\square \to A$, with A an $\mathbb{F}$ algebra, factor through $\overline{R}^\square(\tau)$ in terms of a condition on the corresponding deformation $\rho_A : G_K \to \mathrm{GL}_n(A)$. However, our definition doesn't allow this because it doesn't make sense to attach a Weil–Deligne representation to ρ_A. In other words, $R^\square(\tau)$ is not defined by a moduli interpretation, only $R^\square(\tau)[\frac{1}{l}]$ is.

When $N_\tau = 0$ we can fix this problem. To see why this is possible recall that if $\rho : G_K \to \mathrm{GL}_n(E)$ has Weil–Deligne representation (ρ', N) with $N = 0$ then $\rho' = \rho$ (this was because ρ' was defined by $\rho'(\phi^n x) = \rho(\phi^n x) \exp t(x)N)$). This means that in this case $R^\square(\tau)$ can be defined via a moduli interpretation: conjugate τ so that we have $r_\tau : I_K \to \mathrm{GL}_n(\mathcal{O})$. Then a deformation $\rho_A \in D^\square_{\overline{\rho}}$ corresponding to a map $R^\square \to A$ factors through $R^\square(\tau)$ if and only if

$$\rho_A(x) = r_\tau(x)$$

for every $x \in I_K$. Note however that $R^\square(\tau)$ defined like this might not be reduced or p-torsionfree.

55. Non-scalar examples

We are now going to compute $R^\square(\tau)$ in a number examples. We will assume $\overline{\rho}$ is two dimensional. We begin with the easiest cases where $\overline{\rho}|_{\widetilde{P}_K}$ is non-scalar. Recall that in these cases the computation of $R^\square(\tau)$ was reduced to the calculation of one dimensional deformation rings.

Example 55.1. Suppose that $\theta = \overline{\rho}|_{\widetilde{P}_K}$ is (absolutely) irreducible. Then we showed that

$$R^\square \cong \mathcal{O}[[X, Y, Z_1, Z_2, Z_3]]/((1+X)^{l^a} - 1)$$

where a equals the l-adic valuation of $q-1$. Furthermore, the universal deformation was given by

$$\widetilde{\theta} \otimes \chi^{\mathrm{univ}}$$

where χuniv denotes the universal deformation of the trivial character and $\widetilde{\theta}$: $G_K \to \mathrm{GL}_2(\mathcal{O})$ is an extension to G_K of a lift of θ to $\mathcal{O}$.

First lets look at the irreducible components of $R^\square$. If we assume the coefficients are sufficiently large so that E contains a primitive l^a-th root of unity ζ then

$$(1+X)^{l^a} - 1 = (1+X-\zeta)(1+X-\zeta^2)\dots(1+X-\zeta^{l^a-1})$$

in $\mathcal{O}[X]$. Therefore

$$R^\square \cong \mathcal{O}[[X,Y,Z_1,Z_2,Z_3]]/\prod_{m \nmid l}(1+X-\zeta^m)$$

We see that $\operatorname{Spec} R^\square$ has l^a irreducible components which are determined by which l^a-th root of unity $1+X$ is sent to. Note however that $\zeta \equiv 1$ modulo l so

$$R^\square \otimes_{\mathcal{O}} \mathbb{F} \cong \mathbb{F}[[X,Y,Z_1,Z_2,Z_3]]/X^{l^a}$$

consists of a single (non-reduced) irreducible component.

Let us compute the inertial type of representations on the component $\mathcal{C}_m$ indexed by ζ^m. A morphism $\operatorname{Spec} E' \to \mathcal{C}_m$ corresponds to a map $x : \mathcal{O}[[X,Y,Z_1,Z_2,Z_3]]/(1+X)-\zeta^m \to E'$ and specialising the universal deformation we obtain the representation

$$\widetilde{\theta} \otimes \chi$$

where χ is the character sending $\sigma \mapsto \zeta^m$ and $\phi \mapsto 1+Y$. We see that the restriction of this representation to I_K does not depend upon x and defines an inertial type τ_m. Therefore

$$R^\square(\tau_m) = R^\square/(1+X-\zeta^m)$$

and $R^\square(\tau) = 0$ for any other inertial type. We also note that

$$\overline{R}^\square(\tau_m) = \overline{R}^\square(\tau_{m'})$$

for any m, m'.

Example 55.2. Suppose instead that $\overline{\rho}|_{\widetilde{P}_K} = \theta_1 \oplus \theta_2$ for two characters which are conjugate over G_K. Then

$$R^\square \cong \mathcal{O}[[X,Y,Z_1,Z_2,Z_3]]/((1+X)^{l^b} - 1)$$

where b equals the l-adic valuation of $q+1$ and the irreducible components are indexed by the l^b-th roots of unity. In this case

$$R^\square(\tau) = \mathcal{O}[[X,Y,Z_1,Z_2,Z_3]]/(1+X-\zeta^m)$$

for τ the inertial type $(r_\tau, 0)$ with

$$\begin{aligned} r_\tau &= \operatorname{Ind}_{G_L}^{G_K}(\widetilde{\theta}_1 \otimes \chi)|_{I_K} \\ &= (\widetilde{\theta}_1 \oplus \widetilde{\theta}_2) \otimes \chi|_{I_K} \end{aligned}$$

for χ a character which on inertia sends $\sigma \mapsto \zeta^m$ and $\widetilde{\theta}_1, \widetilde{\theta}_2$ lifts of θ_1, θ_2. Otherwise $R^\square(\tau) = 0$.

Exercise 55.3. Work out the example when $\overline{\rho}|_{\widetilde{P}_K} = \theta_1 \oplus \theta_2$ for non-conjugate characters θ_1, θ_2.

56. Scalar examples

Recall that when $\overline{\rho}|_{\widetilde{P}_K}$ is scalar there can be more complicated behaviour. Twisting by a character we can assume that $\overline{\rho}|_{\widetilde{P}_K}$ is trivial. We begin with an example which illustrates what can happen when types with $N \neq 0$ appear.

Example 56.1. Suppose that $q \not\equiv \pm 1$ and that

$$\overline{\rho}(\sigma) = 1, \qquad \overline{\rho}(\phi) = \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$$

We saw before that

$$R^{\square} \cong \mathcal{O}[[B, P, Q, X, Y]]/(B)(P - Q)$$

and the universal deformation is given by

$$\rho^{\text{univ}}(\sigma) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}$$

$$\rho^{\text{univ}}(\phi) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} q(1+P) & 0 \\ 0 & 1+Q \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}$$

Now there are two components. If we look at the representations where $B \neq 0$ we see that $\rho(I_K)$ is not finite. Therefore, the corresponding inertial type must have $N \neq 0$. Up to twisting by a character there is only one such inertial type given by

$$\tau_{\text{ns}} = (r_{\text{ns}}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix})$$

with $r_{\zeta,\text{ns}}(\sigma) = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta \end{smallmatrix}\right)$. We see that $R^{\square}(\tau_{\text{ns}}) = \mathcal{O}[[B, P, Q, X, Y]]/(P - Q)$. The other possible inertial type is the trivial inertial type $\tau_1 = (\text{Id}, 0)$ and this occurs on the component $B = 0$. Therefore

$$R^{\square}(\tau_1) = \mathcal{O}[[B, P, Q, X, Y]]/B$$

We conclude with an example which illustrates more complicated behaviour.

Example 56.2. Suppose that $\overline{\rho}(\phi)$ has eigenvalues α, β in $\mathbb{F}$ with $\alpha\beta^{-1} \notin \{1, q, q^{-1}$. Then we computed that

$$R^{\square} \cong \mathcal{O}[[A, B, P, Q, X, Y]]/((1 + X_1)^{l^a} - 1, (1 + X_2)^{l^a} - 1)$$

Furthermore we showed that ρ^{univ} was given by

$$\rho^{\text{univ}}(\sigma) = \begin{pmatrix} 1+P & 0 \\ 0 & 1+Q \end{pmatrix}, \qquad \rho^{\text{univ}}(\phi) = \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha + A & 0 \\ 0 & \beta + B \end{pmatrix} \begin{pmatrix} 1 & X \\ Y & 1 \end{pmatrix}$$

We see that the irreducible components are indexed by ordered pairs of l^a-th roots of unity ζ_1, ζ_2. Note that any specialisation of ρ^{univ} to E'/E has finite image of inertia. Therefore, the only inertial types appearing have $N = 0$. The inertial type of the component with $\zeta_1 = \zeta_2 = \zeta$ (which we denote τ_ζ)does not equal the inertial type of any other component so

$$R^{\square}(\tau_\zeta) \cong \mathcal{O}[[A, B, P, Q, X, Y]]/(1 + P - \zeta, 1 + Q - \zeta)$$

On the other hand, if $\zeta_1 \neq \zeta_2$ then the inertial type τ_{ζ_1,ζ_2} on the (ζ_1,ζ_2) component equals the inertial type on the (ζ_2,ζ_1) component. It follows that $R^\square(\tau_{\zeta_1,\zeta_2})$ can be defined by two equations $1+P+1+Q = \zeta_1+\zeta_2$ and $PQ = \zeta_1\zeta_2$. Thus

$$R^\square(\tau_{\zeta_1,\zeta_2}) = \mathcal{O}[[A,B,P,Q,X,Y]]/(2+P+Q-\zeta_1-\zeta_2, PQ-\zeta_1\zeta_2) \cong \mathcal{O}[[A,B,X,Y,P]]/(1+P-\zeta_1)(1+P-\zeta_2)$$

We have $R^\square(\tau) = 0$ for all other τ. Reducing modulo l we see that their is a difference between $\overline{R}^\square(\tau_\zeta)$ and $\overline{R}^\square(\tau_{\zeta_1,\zeta_2})$ because

$$\overline{R}^\square(\tau_\zeta) \cong \mathbb{F}[[A,B,X,Y]]$$

is reduced while

$$\overline{R}^\square(\tau_{\zeta_1,\zeta_2}) \cong \mathbb{F}[[A,B,P,X,Y]]/(P^2)$$

is not reduced.

Part 3. **Lecture 25**

57. Cycles

Recall the following example from last lecture:

Example 57.1. In our usual $l \neq p$ situation we have $R^\square = R^\square_{\overline{\rho}} \otimes_{W(\mathbb{F})} \mathcal{O}$ and for each inertial type τ defined other $E = \mathcal{O}[\frac{1}{p}]$ we have quotients

$$R^\square(\tau)$$

of $R^\square$. Suppose $\overline{\rho}_{\overline{P}_K}$ is trivial and that $\overline{\rho}(\phi)$ has eigenvalues α,β with $\alpha\beta^{-1} \notin \{1,q,q^{-1}\}$. Then

$$R^\square = \mathcal{O}[[X,Y,P,Q,A,B]]/((1+X)^{l^a}-1,(1+Y)^{l^a}-1)$$

and $R^\square(\tau) = 0$ unless $\tau = (r_{\zeta_1,\zeta_2},0)$ with $r_{\zeta_1,\zeta_2}(\sigma) = \left(\begin{smallmatrix}\zeta_1 & 0\\ 0 & \zeta_2\end{smallmatrix}\right)$ for l^a-th roots of unity ζ_1,ζ_2. We computed that

$$R^\square(\tau_{\zeta_1,\zeta_2} = \begin{cases}\mathcal{O}[[X,Y,P,Q,A,B]]/(1+X+1+Y-\zeta_1-\zeta_2,(1+X)(1+Y)-\zeta_1\zeta_2) & \text{if } \zeta_1 \neq \zeta_2\\ \mathcal{O}[[X,Y,P,Q,A,B]]/(1+X-\zeta_1,1+Y-\zeta_2) & \text{if } \zeta_1 = \zeta_2\end{cases}$$

Set $\overline{R}^\square = R^\square \otimes_{\mathcal{O}} \mathbb{F}$. Then $\overline{R}^\square \cong \mathbb{F}[[X,Y,P,Q,A,B]]/(X^{l^a},Y^{l^a})$ and

$$\overline{R}^\square(\tau_{\zeta_1,\zeta_2}) = \begin{cases}\mathbb{F}[[X,Y,P,Q,A,B]]/(X+Y,XY) & \text{if } \zeta_1 \neq \zeta_2\\ \mathbb{F}[[X,Y,P,Q,A,B]]/(X,Y) & \text{if } \zeta_1 = \zeta_2\end{cases}$$

Clearly these two rings are very different; the first is non-reduced (since $X+Y = 0$ we have $XY = -X^2 = 0$) while the second is a power series ring. We want to give a precise way of measuring this difference.

Recollection 57.2. Recall that if $X = \operatorname{Spec} A$ is an affine scheme then there is an associated topological space $|X| = \{\text{prime ideals} \in A\}$. The following sets are in bijection:

(1) closed subsets of $|X|$.
(2) reduced closed subschemes of X.

(3) radical ideals $I \subset R$ (recall an ideal is radical if $a^n \in I$ implies $a \in I$. This is the same as asking that R/I is reduced).

On the other hand, the set of closed subschemes in X are in bijection with ideals in R, so there are many more closed subschemes than closed subsets. In our previous example we see that

$$|\operatorname{Spec} R^{\square}| = |\operatorname{Spec} R^{\square}(\tau_{\zeta_1,\zeta_2})| = |\operatorname{Spec} R^{\square}(\tau_{\zeta,\zeta})|$$

but only is reduced.

Recollection 57.3. For an affine scheme $X = \operatorname{Spec} A$ and $J \subset |X|$ closed recall that the following are equivalent:

(1) J is irreducible
(2) one cannot write $J = J_1 \cup J_2$ for $J_i \subset J$ proper closed subschemes
(3) If J corresponds to the radical ideal $I \subset A$ then I is a prime ideal.

Definition 57.4. Let $X \operatorname{Spec} A$ be a Noetherian affine scheme. For every $n \geq 0$ define the group of n-dimensional cycles in X

$$Z_n(X)$$

as the free abelian group on the set of prime ideals $\mathfrak{p}$ in X such that $\operatorname{Spec} A/\mathfrak{p}$ has dimension n. Therefore, an element of $|X|$ can be written as a finite sum

$$\sum n_{\mathfrak{p}} \mathfrak{p}$$

for $n_{\mathfrak{p}} \in \mathbb{Z}$. Since prime ideals correspond to irreducible closed subsets in $|X$ we could equivalently define $Z_n(X)$ as the free abelian group on the set of n-dimensional irreducible closed subsets. Note this definition also makes sense without X being affine.

Construction 57.5. For any closed subscheme $Y \subset X = \operatorname{Spec} A$ we can define an element

$$[Y] \in Z_n(X)$$

as follows: since X is Noetherian we can write $|Y| = \bigcup |Y_i|$ for $|Y_i| \subset |X|$ irreducible subsets. Assume $Y_1, \ldots, Y_m$ are those irreducible subsets of dimension n, and write $\mathfrak{p}_i$ for the corresponding prime ideal. Then we define

$$[Y] = \sum_{i=1}^{n} \operatorname{mult}(Y, \mathfrak{p}_i)\mathfrak{p}_i$$

where

$$\operatorname{mult}(Y, \mathfrak{p}_i) = \operatorname{length}(A/I)_{\mathfrak{p}_i}$$

is the length of $(A/I)_{\mathfrak{p}_i}$ as a module over itself. Note this is the same thing as the dimension

Example 57.6. Take $X = \operatorname{Spec} \overline{R}^{\square}$ from before. Let us compute the elements $[\operatorname{Spec} \overline{R}^{\square}(\tau_{\zeta_1,\zeta_2})] \in Z_4(X)$. Note that $\overline{R}^{\square}$ contains a single irreducible component (of dimension 4) corresponding to the prime ideal generated by $\mathfrak{p} = (X, Y)$. Since $\overline{R}^{\square} = \mathbb{F}[[X, Y, P, Q, A, B]]/(X^{l^a}, Y^{l^a})$ we have

Since $\overline{R}^{\square}(\tau_{\zeta,\zeta}) = \overline{R}^{\square}/\mathfrak{p}$ we have

$$\overline{R}^{\square}_{\mathfrak{p}} = \mathbb{F}((A,B,P,Q))[[X,Y]]/(X^{l^a},Y^{l^a})$$

so

$$[X] = l^{2a}\mathfrak{p}$$

On the other hand we have $\overline{R}^{\square}(\tau_{\zeta,\zeta}) = \overline{R}^{\square}/\mathfrak{p}$ and so $\overline{R}^{\square}(\tau_{\zeta,\zeta}) = \mathbb{F}((A,B,P,Q))$, and

$$[\operatorname{Spec}\overline{R}^{\square}(\tau_{\zeta,\zeta})] = \mathfrak{p}$$

For $\zeta_1 \neq \zeta_2$ we have $\overline{R}^{\square}(\tau_{\zeta_1,\zeta_2}) = \overline{R}^{\square}/(XY, X+Y)$. As $\overline{R}^{\square}_{\mathfrak{p}} = \mathbb{F}((A,B,P,Q))[[X,Y]]/(XY,X+Y)$ we have

$$[\operatorname{Spec}\overline{R}^{\square}(\tau_{\zeta_1,\zeta_2})] = 2[X]$$

Cycles don't see everything.

Example 57.7. Suppose $R = \mathbb{F}[[X,Y]]$ and consider the closed subscheme $Y = \operatorname{Spec} R/(XY,Y^2)$ in $\operatorname{Spec} R$. Even though Y is not reduced we claim that

$$[Y] = \mathfrak{p} \in Z_1(\operatorname{Spec} R)$$

for $\mathfrak{p}$ the prime ideal (Y). To see this note that $\mathfrak{p}$ is the unique minimal prime of $R' = R/(XY,Y^2)$. Localising R' at $\mathfrak{p}$ involves inverting all elements not divisible by Y. In particular, we invert X and so $Y = 0$ in $R'_{\mathfrak{p}}$. Hence

$$R'_{\mathfrak{p}} = \mathbb{F}((X))$$

which shows the claim.

Lemma 57.8. *Suppose that $Y \subset X$ is equidimensional of dimension n and suppose that*

$$[Y] = \sum_Z [Z]$$

with the sum running over closed irreducible subsets. In other words, assume the multiplicity of every component in Y is one. Then there exists an open subscheme $U \subset Y$ such that U is reduced. Conversely, if Y is generically reduced then every component of Y has multiplicity one.

58. $l \neq p$ Breuil–Mézard conjecture

We can now state the $l \neq p$ Breuil–Mézard conjecture. For this we return to our usual set-up: $K/\mathbb{Q}_p$ is a finite extension and so is $E/\mathbb{Q}_l$. Here $l \neq p$ and $\mathcal{O}$ denotes the ring of integers in E and $\mathbb{F}$ the residue field. Fix $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F})$ and set

$$R^{\square} = R^{\square}_{\overline{\rho}} \otimes_{W(\mathbb{F})} \mathcal{O}$$

Theorem 58.1 (Shotton)**.** *Assume $l \neq 2$. Let k denote the residue field of K. Then, for each irreducible representation $\theta : \mathrm{GL}_2(\mathbb{F}(k) \to \mathrm{GL}_2(\mathbb{F})$, there exists*

$$\mathcal{C}(\theta) \in Z^4(\overline{R}^{\square})$$

with the following property: For any inertial type $\tau = (r_\tau, 0)$ defined over E, one has

$$[\operatorname{Spec} \overline{R}^{\square}(\tau)] = \sum_{\theta} m(\theta,\tau)\mathcal{C}(\theta)$$

where $m(\theta,\tau)$ denotes the multiplicity of θ inside the reduction modulo l of the representation

$$\sigma(\tau)$$

attached to τ via the inertial Langlands correspondence. For the inertial type $\tau = (r_\tau, N_\tau)$ with $N_\tau \neq 0$ one has

$$[\operatorname{Spec} \overline{R}^{\square}(\tau)] + [\operatorname{Spec} \overline{R}^{\square}(\tau')] = \sum_{\theta} m(\theta,\tau)\mathcal{C}(\theta)$$

where $\tau = (r_\tau, 0)$.

An identical result also holds in dimension > 2 except that one then considers n^2-dimensional cycles.

59. Inertial Langlands correspondence

The classical local Langlands correspondence (for GL_2) defines a bijection between isomorphism classes of two dimensional Weil–Deligne representations and smooth irreducible admissible two dimensional representations of $\mathrm{GL}_2(K)$ on $\overline{\mathbb{Q}}_l$-vector spaces. Actually, one has to restrict to Frobenius semi-simple Weil–Deligne representations on the Galois side (a WD-representation (ρ', N) is Frobenius semi-simple if $\rho'(\phi)$ can be diagonalised). This bijection should satisfy a number of conditions. Let us write

$$\operatorname{rec}(\pi)$$

for the WD-rep corresponding to an irreducible admissible π. Note that here we suppress many additional choices and normalisations.

Theorem 59.1. *If $\tau = (r_\tau, N_\tau)$ is an inertial type then there exists a unique finite dimensional representation $\sigma(\tau)$ over $\overline{\mathbb{Q}}_l$ of $\mathrm{GL}_2(\mathcal{O}_K)$ such that for all irreducible admissible π one has*

$$\pi|_{\mathrm{GL}_2(\mathcal{O}_K)} \text{ contains } \sigma(\tau) \Rightarrow \operatorname{rec}(\pi)|_{I_K} \cong r_\tau \text{ and either } N \cong N_\tau \text{ or } N_\tau \neq 0 \text{ and } N = 0$$

If π is infinite dimensional then the converse is also true.

In the two dimensional case one constructs rec by classifying these isomorphism classes on either side and showing that they match. This allows us to define $\sigma(\tau)$ by the following explicit formula:

- if $\tau = (1,0)$ then $\sigma(\tau)$ is the trivial representation.
- if $\tau = (1,N)$ with $N = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ then $\sigma(\tau)$ is (the inflation to $\mathrm{GL}_2(\mathcal{O}_K)$ of) the Steinberg representation of $\mathrm{GL}_2(k)$.
- If $\tau = (1 \oplus \epsilon, 0)$ for $\epsilon : K^\times \to \overline{\mathbb{Q}}_l^\times$ non-trivial of exponent N (i.e the smallest N such that $\epsilon|_{1+\mathfrak{m}_K^N}$ is trivial) then

$$\sigma(\tau) = \operatorname{Ind}_{K_0(N)}^{\mathrm{GL}_2(\mathcal{O}_K)} \epsilon$$

where $K_0(N)$ consists of matrices upper triangular modulo $\mathfrak{m}_K^N$. Here we view ϵ as a representation of the Weil group via local class field theory.

- If $\tau = (r_\tau, 0)$ with r_τ irreducible then $r_\tau = \mathrm{rec}(\pi)|_{I_K}$ for a cuspidal π. Any such π can be written as
$$\text{c-Ind}_J^{\mathrm{GL}_2(K)} \Lambda$$
for J a certain subgroup which contains the center of $\mathrm{GL}_2(K)$ and is compact modulo this center. Then
$$\sigma(\tau) = \mathrm{Ind}_{J^0}^{\mathrm{GL}_2(\mathcal{O}_K)} \Lambda|_{J^0}$$
where $J^0 \subset J$ is the maximal compact subgroup.

60. A brief look at the $l = p$ Breuil–Mézard conjecture

Now suppose $l = p$. We would like a similar statement comparing cycles in $\operatorname{Spec} \overline{R}^\square$ using the representation theory of $\mathrm{GL}_n(k)$ and (some elements of) the Langlands correspondence.

Remark 60.1. When $l \neq p$ the rings has dimension n^2. However, we really should be considering them moduli the action of conjugation by GL_n. Usually this quotient would give a stack rather than a scheme, of dimension
$$n^2 - n^2 = 0$$
This illustrates that one should think of these inertial types as discrete parameters. When $l = p$ we will see that there are also continuous parameters appearing.

Remark 60.2. Historically the $l = p$ version of the Breuil–Mézard conjecture came first. The motivation was that it could be used to prove modularity lifting theorems, and when $l \neq p$ one was already able to understand the situation well enough that the $l \neq p$ Breuil–Mézard conjecture was not necessary from this point of view. In fact Shotton's proof of the $l \neq p$ conjecture for GL_n reverse engineered these ideas, and used existing modularity lifting theorems.

,

- The first step would be to obtain an analogue of $\overline{R}^\square(\tau)$ when $l = p$. Unlike in the $l \neq p$ case one cannot attach a WD-rep to any p-adic representation $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$. Instead one has a to restrict attention to a certain class of de Rham representations (this turns out not to be so bad because every representation coming from nature, i.e. from geometry is de Rham). Then one has a fully faithful functor
$$\{\text{de Rham representation}\} \to \{(\rho', N, \mathrm{Fil})\}$$
into the category of pairs of WD-reps together with a choice of filtration (where the filtration measures the Hodge–Tate weights of the de Rham representation). This motivates us to consider quotients $R^\square(\tau, \mu)$ of $R^\square$ for τ an inertial type and μ an isomorphism class of filtration.

- These quotients should be defined by the property that $x : R^{\square} \to E$ factors through $R^{\square}(\tau,\mu)$ if and only ρ_x corresponds to (τ,μ) under the above functor. Unlike in the $l \neq p$ case, it is very unclear whether these quotients should exist. In fact, it was an open problem for a long time, until Kisin gave a construction around 2005.
- One can compute the dimensions of $R^{\square}(\tau,\mu)$ to be
$$n^2 + d(\mu)$$
where $d(\mu)$ denotes the dimension of the flag variety classifying filtrations of type μ. The largest possible value of $d(\mu)$ is $n(n-1)/2$ and when this occurs we say that μ is regular.

Conjecture 60.3. *For each irreducible $\mathbb{F}$-representation θ of $\mathrm{GL}_n(k)$ there exist cycles*
$$\mathcal{C}(\theta) \in Z^{n^2+n(n-1)/2}(\operatorname{Spec} \overline{R}^{\square})$$
such that for any regular μ one has
$$[\operatorname{Spec} \overline{R}(\tau,\mu)] = \sum m(\theta,\tau,\mu)\mathcal{C}(\theta)$$
where $m(\theta,\tau,\mu)$ denotes the multiplicity of θ inside
$$\overline{\sigma}(\tau,\mu)$$
where $\overline{\sigma}(\tau,\mu)$ is the base change of $\mathbb{F}$ of a lattice inside $\sigma(\tau,\mu) := \sigma(\tau) \otimes V(\mu)$ where $V(\mu)$ denotes the algebraic representation of GL_n with highest weight μ (or $\mu - \rho$ where $\rho = (n-1, n-2, \ldots, 1, 0)$).

This is known when $n = 2$ and $K = \mathbb{Q}_p$ by work of Kisin and Paskunas, and others. Besides a few other special cases essentially nothing is known otherwise. Also nothing is known (not even a conjecture) or what happens when μ is not regular.

References